N° 4573

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale
le 2 mars 2017.

N° 448

SÉNAT

SESSION ORDINAIRE DE 2016-2017

Enregistré à la Présidence du Sénat
le 2 mars 2017.

DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

RAPPORT

*relatif à l'***activité** *de la* **délégation parlementaire au renseignement pour l'année 2016**

Par

MME Patricia ADAM,

Députée

Déposé sur le Bureau de l'Assemblée nationale
par Mme Patricia ADAM

Présidente de la Délégation.

Déposé sur le Bureau du Sénat
par M. Philippe BAS

Premier vice-président de la Délégation.

SOMMAIRE

—

Pages

Mesdames, Messieurs,

Depuis deux ans, la France est endeuillée par une série d'attentats terroristes commis et revendiqués par des activistes favorables à l'idéologie islamiste radicale et djihadiste, dans le prolongement de ceux ayant frappé notre pays en 2012.

Cette terrible réalité ne doit pas pour autant occulter les résultats obtenus par ailleurs par nos services de renseignement et de sécurité : ils sont en effet parvenus à déjouer une vingtaine de tentatives d'attentats depuis le début de l'année 2016.

La politique publique du renseignement constitue la première ligne de défense de notre pays face à la menace terroriste. C'est la raison pour laquelle les moyens, tant matériels que juridiques, dont disposent les services de renseignement ont fait l'objet de renforcements successifs, parallèlement à un accroissement des garanties accordées aux citoyens. Celles-ci s'exercent notamment au travers du contrôle parlementaire.

La Délégation parlementaire au renseignement, créée par la loi n° 2007-1443 du 9 octobre 2007, a ainsi vu ses compétences renforcées par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019. Elle assure le contrôle parlementaire et l'évaluation de l'action du Gouvernement en matière de renseignement. Ses travaux sont couverts par le secret de la défense nationale. Sa fonction consiste, pour partie, à effectuer des recommandations à destination de l'exécutif à partir de l'analyse de la politique suivie et du fonctionnement des services. À cet effet, elle rend un rapport comportant des informations classifiées au Président de la République, au Premier ministre et aux Présidents des deux assemblées. Elle publie le même rapport (mais sans les informations classifiées) après qu'il a été présenté officiellement au Président de la République.

Au cours de l'année écoulée, pour définir ses orientations et pour élaborer ses prescriptions, la Délégation parlementaire au renseignement a accompli un important travail d'information.

Elle a procédé à près de 75 heures d'entretiens. Elle a entendu les ministres de la Défense et de la Justice, ainsi que le directeur de cabinet du Premier ministre. Elle a auditionné les principaux responsables de la politique du renseignement et les directeurs de service en charge de sa mise en œuvre. Elle s'est déplacée en Belgique pour rencontrer le Comité permanent de contrôle des services de renseignement et de sécurité (Comité permanent R) et la commission chargée de l'accompagnement de ce Comité au sein de la Chambre des représentants. Enfin, elle a reçu en France une délégation de membres du Congrès américain présidée par le Président du Comité du renseignement du Sénat, une délégation de représentants du G 10 allemand – c'est-à-dire de l'instance qui,

outre-Rhin, exerce les mêmes fonctions que la Commission nationale du contrôle des techniques de renseignement (CNCTR) –, une délégation du Comité parlementaire italien pour la sécurité de la République (COPASIR) et une délégation du Comité parlementaire britannique chargé de superviser les activités de renseignement et de sécurité (« Intelligence and Security Committee »).

La synthèse des travaux de la Délégation figure dans le présent rapport. Ce dernier s'articule selon les quatre axes de réflexion suivants :

– le bilan d'activité de la Délégation en 2016 et le suivi de ses propositions antérieures (I) ;

– les grands aspects de la politique du renseignement en 2015 et en 2016 (II) ;

– la communauté du renseignement en 2015 et en 2016, et les préconisations de la Délégation face à certains problèmes qu'elle rencontre (III) ;

– enfin, l'analyse des lois du 24 juillet 2015 relative au renseignement et du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, ainsi que leur évaluation au terme d'une année d'application (IV).

En outre, le lecteur pourra trouver, en chapitre V, une présentation des travaux de la Commission de vérification des fonds spéciaux (CVFS), établie par son président, M. le sénateur François-Noël Buffet, et portant sur l'exercice 2015.

De manière générale, dans les différentes parties du présent rapport, la Délégation a estimé que la politique du renseignement devait répondre à six grands principes :

– la poursuite du renforcement des moyens accordés aux différents services et amorcé avec le Livre blanc sur la défense et la sécurité nationale de 2008 ;

– l'amélioration de la capacité de recueillir les renseignements au plus près du terrain – ce qui suppose de renforcer, notamment, le renseignement territorial et le renseignement pénitentiaire ; il faut également renforcer les échelons régionaux des services, échelons qui jouent un rôle essentiel dans la remontée des informations et dans la captation des « signaux faibles » ;

– l'enrichissement, sur certains points, des deux lois de 2015 sur le renseignement et sur la surveillance des communications électroniques internationales ;

– la recherche d'une efficacité maximale des services en levant certains obstacles qui peuvent leur poser problème ;

– la réaffirmation de l'ensemble des finalités de la politique du renseignement ; c'est ainsi qu'indépendamment de la lutte antiterroriste, il ne faut pas oublier les autres finalités du renseignement – à savoir la défense de l'indépendance nationale ; la défense de l'intégrité du territoire ; la préservation des intérêts majeurs de la politique étrangère ; la prévention de toute forme d'ingérence étrangère ; la préservation des intérêts économiques, industriels et scientifiques majeurs ; la prévention des atteintes à la forme républicaine des institutions ; la prévention des actions visant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 du code de la sécurité intérieure ; la prévention des violences collectives de nature à porter gravement atteinte à la paix publique ; la prévention de la criminalité et de la délinquance organisées ; et la lutte contre la prolifération des armes de destruction massive ;

– enfin, la nécessité de disposer d'un système d'évaluation performant de la politique du renseignement.

On retrouvera toutes ces observations dans les développements qui suivent.

I. LE BILAN D'ACTIVITÉ DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT EN 2016 ET LE SUIVI DE SES PROPOSITIONS ANTÉRIEURES

La Délégation parlementaire au renseignement et la Commission de vérification des fonds spéciaux ont connu une évolution sensible de leurs activités à partir de l'année 2013. Ainsi, la DPR qui, jusqu'à cette date n'avait pour mission que *« le suivi de l'activité générale des services de renseignement »* est-elle désormais chargée, aux termes de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, du *« contrôle et de l'évaluation de l'action du Gouvernement en matière de renseignement »*.

Par ailleurs, à la même date, la CVFS a été intégrée au sein de la DPR en tant que *« formation spécialisée »*. Ses membres en sont issus et elle présente chaque année son rapport à la Délégation. Cette mesure permet, d'une part, de mutualiser les secrétariats et, d'autre part, d'assurer à la DPR une meilleure visibilité sur l'ensemble des crédits dont disposent les différents services de renseignement.

Enfin, la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a consolidé ces évolutions en fixant un cadre juridique plus complet et plus cohérent, tant pour les activités des services de renseignement que pour celles des différentes instances chargées de les contrôler, dont la DPR.

Celle-ci en a largement inspiré le contenu par les recommandations de ses rapports successifs, et bénéficie désormais de moyens d'information accrus.

Le présent chapitre sera organisé en trois grandes parties : tout d'abord, on détaillera le mode de fonctionnement de la DPR ; ensuite, on indiquera quels ont été les travaux réalisés par la Délégation au cours de l'année 2016 et au début de l'année 2017 ; enfin, on fera un point sur l'application, au cours de l'année écoulée, des recommandations de la DPR formulées en 2014 et en 2015.

A. LE MODE DE FONCTIONNEMENT DE LA DPR

Un rappel est utile concernant la composition de cette délégation, les moyens d'information dont elle dispose et les procédures par lesquelles elle fait connaître ses réflexions et ses recommandations.

1. Composition de la DPR

La Délégation parlementaire au renseignement a été créée en 2007 (par la loi n° 2007-1143 du 9 octobre 2007 portant création d'une Délégation parlementaire au renseignement : article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires). Ses

missions ont été étendues en 2013 par la loi de programmation militaire pour 2014-2019.

Elle est composée de quatre députés et de quatre sénateurs, dont les quatre présidents des commissions de la Défense et des Lois des deux assemblées, membres de droit.

En 2016, ses membres sont les suivants :

– pour l'Assemblée nationale : Mme Patricia Adam, ***Présidente de la Délégation***, Présidente de la commission de la Défense nationale et des forces armées ; M. Jacques Myard, désigné par le Président de l'Assemblée nationale ; M. Philippe Nauche, désigné par le Président de l'Assemblée nationale ; et M. Dominique Raimbourg, ***deuxième Vice-Président de la Délégation***, Président de la commission des Lois ;

– pour le Sénat : M. Philippe Bas, ***premier vice-président de la Délégation***, Président de la commission des Lois ; M. Michel Boutant, désigné par le Président du Sénat ; M. François-Noël Buffet, désigné par le Président du Sénat ; et M. Jean-Pierre Raffarin, Président de la commission des Affaires étrangères, de la défense et des forces armées.

Créée par l'article 154 de la loi de finances pour 2002 et devenue formation spécialisée de la DPR au titre de l'article 13 de la loi de programmation militaire pour 2014-2019, la CVFS comporte quatre membres : deux députés et deux sénateurs, issus de la Délégation, et désignés de façon à assurer une représentation pluraliste. Le président de la Commission est désigné chaque année par la Délégation. Soucieuse d'un bon équilibre institutionnel, la Délégation a pris le parti de désigner un sénateur pour présider la CVFS lorsque la DPR est présidée par un député et *vice versa*.

En 2016, les membres de la CVFS sont MM. Jacques Myard et Philippe Nauche pour l'Assemblée nationale ; MM. Michel Boutant et François-Noël Buffet, ***Président de la Commission***, pour le Sénat.

Tous les membres de la DPR et de la CVFS sont habilités ès-qualités au secret de la défense nationale.

2. Moyens d'information

Pour son information, la Délégation peut entendre un certain nombre de personnalités dont la liste figure à l'article 6 *nonies* de l'ordonnance du 27 novembre 1958 et elle reçoit communication d'un certain nombre de documents visés par le même texte.

Ainsi, elle peut auditionner :

– le Premier ministre ;

– les ministres concernés par les questions de renseignement – tout particulièrement ceux de la Défense, de l'Intérieur, de l'Économie, des Finances et du Budget, qui disposent de l'autorité hiérarchique sur les services spécialisés de renseignement ;

– le Secrétaire général de la défense et de la sécurité nationale ;

– le Coordonnateur national du renseignement ;

– le directeur de l'Académie du renseignement ;

– les directeurs en fonction des différents services de renseignement, accompagnés des collaborateurs de leur choix, en fonction de l'ordre du jour de la Délégation, ainsi que toute personne placée auprès de ces directeurs et occupant un emploi pourvu en Conseil des ministres ;

– les directeurs d'administration centrale ayant à connaître des activités des services.

S'agissant de l'application de la loi du 24 juillet 2015 relative au renseignement, elle peut entendre le Premier ministre chaque semestre et également les personnes spécialement déléguées par celui-ci pour délivrer des autorisations de mise en œuvre de techniques de renseignement.

Elle peut également inviter :

– le président de la Commission nationale du contrôle des techniques de renseignement (CNCTR) pour que ce dernier lui présente le rapport d'activité de la Commission, ainsi que les observations que la Commission adresse au Premier ministre en application de l'article L. 833-10 du code de la sécurité intérieure et les avis que la Délégation demande à la Commission en application de l'article L. 833-11 du même code ;

– le président de la Commission consultative du secret de la défense nationale (CCDSN) pour qu'il lui présente le rapport d'activité de la Commission.

Par ailleurs, la DPR reçoit ou se fait communiquer :

– la stratégie nationale du renseignement ;

– des éléments d'information issus du Plan national d'orientation du renseignement ;

– le rapport annuel exhaustif des crédits consacrés au renseignement ;

– le rapport annuel d'activité des services de renseignement (il s'agit d'une novation et le premier rapport d'activité a été communiqué, cette année, au début du mois de novembre à la DPR par le Coordonnateur national du renseignement) ;

– des éléments d'appréciation relatifs à l'activité générale et à l'organisation des services de renseignement (il s'agit des services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure et des services autorisés par le décret en Conseil d'État 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 dudit code) ;

– des observations que la CNCTR adresse au Premier ministre en application de l'article L. 833-10 du code de la sécurité intérieure ainsi qu'une présentation, par technique et par finalité, des éléments statistiques figurant dans le rapport d'activité mentionné à l'article L. 833-9 du même code.

Elle peut solliciter du Premier ministre la communication de tout ou partie des rapports de l'Inspection des services de renseignement (ISR), ainsi que des rapports des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence.

Enfin, la DPR peut effectuer des déplacements, en France ou à l'étranger, pour compléter son information. Par exemple, elle s'est rendue en Belgique, au cours du mois d'avril 2016, pour rencontrer le Comité permanent de contrôle des services de renseignement et de sécurité (Comité permanent R), ainsi que la commission chargée de l'accompagnement de ce Comité au sein de la Chambre des représentants.

3. Procédures par lesquelles la DPR fait connaître ses évaluations

La DPR publie un rapport d'activité chaque année. Ce rapport, qui peut contenir des informations classifiées, est secret et ses destinataires sont exclusivement le Président de la République, le Premier ministre et les Présidents des deux assemblées. Les membres de la DPR présentent leurs travaux et leurs conclusions au Président de la République au cours d'une réunion de travail qui se tient à l'Élysée.

La DPR publie également un rapport annuel public destiné à l'ensemble des citoyens. Le rapport public 2014 a donné lieu, pour la première fois, à un débat en séance publique à l'Assemblée nationale le 10 février 2015. Par ailleurs, le rapport public 2015 a donné lieu à une communication au sein de la commission des Affaires étrangères, de la défense et des forces armées du Sénat le 15 février 2016.

Dans ces deux documents, la DPR adresse des recommandations aux pouvoirs publics (103 en 2014 et 29 en 2015). Elle suit leur application tout au long de l'année et, tout particulièrement, au moment de la rédaction du rapport annuel de l'année suivante.

B. LES TRAVAUX CONDUITS PAR LA DÉLÉGATION EN 2016 ET EN 2017

Au cours de l'année 2016 et au début de l'année 2017, le calendrier des réunions et des déplacements de la Délégation parlementaire au renseignement a été le suivant :

➢ **Réunion du 18 février 2016**

• Audition de M. Didier Le Bret, Coordonnateur national du renseignement, accompagné de Mme Agnès Deletang, magistrat, conseiller juridique.

• Audition de M. Philippe Hayez, magistrat à la Cour des comptes, enseignant à l'Institut d'études politiques de Paris.

• Audition de M. Loïc Garnier, chef de l'Unité de coordination de la lutte antiterroriste (UCLAT).

➢ **Déplacement du 3 mars 2016**

• Déplacement à la Direction générale de la sécurité intérieure (DGSI) et visite de la cellule INTERSERVICES.

➢ **Réunion du 22 mars 2016**

• Entretien avec une délégation du Congrès américain conduite par M. Richard Burr, sénateur et Président du Comité du renseignement du Sénat.

➢ **Réunion du 24 mars 2016**

• Audition de M. le préfet Olivier de Mazières, chef de l'État-major opérationnel de prévention du terrorisme (EMOPT).

• Audition de M. Jean-Paul Garcia, Directeur national du renseignement et des enquêtes douanières (DNRED).

➢ **Déplacement du 7 avril 2016**

• Déplacement au ministère de la Défense et visite de la cellule HERMES.

• Entretien avec le général de corps d'armée Christophe Gomart, Directeur du renseignement militaire (DRM).

➢ **Déplacement du 28 avril 2016**

• Déplacement à Bruxelles, visite du Comité R et de la commission chargée de l'accompagnement de ce Comité au sein de la Chambre des représentants.

➢ **Réunion du 3 mai 2016**

• Audition de M. Bernard Bajolet, Directeur général de la sécurité extérieure.

➢ **Réunion du 26 mai 2016**

• Audition de M. Bruno Dalles, Directeur de Tracfin.

• Audition de M. le général de corps d'armée Jean-François Hogard, Directeur de la protection et de la sécurité de la défense (DPSD) [(1)].

• Audition de M. le général de corps d'armée Michel Pattin, représentant le Directeur général de la Gendarmerie nationale, Directeur des opérations et de l'emploi, auquel est rattachée la Sous-direction de l'anticipation opérationnelle (SDAO).

➢ **Réunion du 9 juin 2016**

• Audition de Mme Lucile Dromer-North, Directrice de l'Académie du renseignement.

➢ **Réunion du 16 juin 2016**

• Audition de M. Bernard Bajolet, Directeur général de la sécurité extérieure,

• Audition de M. Jérôme Léonnet, Directeur central adjoint de la sécurité publique en charge du renseignement, chef du Service central du renseignement territorial (SCRT).

➢ **Réunion du 28 juin 2016**

• Audition de M. Jean-Yves Le Drian, ministre de la Défense.

➢ **Réunion du 29 juin 2016**

• Audition de M. Patrick Calvar, Directeur général de la sécurité intérieure.

➢ **Déplacement du 12 juillet 2016**

• Visite du Groupement interministériel de contrôle (GIC).

• Entretien avec M. l'ingénieur général de l'armement Pascal Chauve, directeur du GIC.

---

(1) Devenue Direction du renseignement et de la sécurité de la défense (décret n° 2016-1337 du 7 octobre 2016).

➢ **Réunion du 27 septembre 2016**

• Entretien avec cinq membres de la commission G 10 rattachée au Bundestag de la République fédérale d'Allemagne : M. Hans-Joachim Hacker (député), M. Frank Hofmann, M. Bertold Huber, M. Andreas Schmidt et M. Wolfgang Wieland (député).

➢ **Réunion du 13 octobre 2016**

• Audition de M. Jean-Baptiste Carpentier, Commissaire à l'information stratégique et à la sécurité économiques.

➢ **Réunion du 27 octobre 2016**

• Audition de M. Christian Protar, contrôleur général des armées, Secrétaire général de l'Inspection des services de renseignement,

• Audition de M. Bernard Bajolet, Directeur général de la sécurité extérieure, accompagné de M. Patrick Pailloux, Directeur technique de la DGSE.

➢ **Réunions du 3 novembre 2016**

– Dans la matinée :

• Audition de M. Yann Jounot, Coordonnateur national du renseignement, accompagné de Mme Agnès Deletang, magistrat, conseiller juridique.

• Audition de M. Renaud Vedel, conseiller au cabinet de M. le Premier ministre, accompagné de M. Cyrille Chabauty, Délégué du Premier ministre pour l'autorisation de mise en œuvre des techniques de renseignement.

– Dans l'après-midi :

• Audition de M. Jean-Claude Mallet, conseiller spécial de M. le ministre de la Défense, accompagné de Mme Claire Landais, Directrice des Affaires juridiques du ministère.

➢ **Réunion du 17 novembre 2016**

• Audition de M. Jean-Claude Mallet, conseiller spécial de M. le ministre de la Défense, accompagné de Mme Claire Landais, Directrice des Affaires juridiques du ministère.

➢ **Réunion du 23 novembre 2016**

• Audition de M. Francis Delon, Président de la Commission nationale du contrôle des techniques de renseignement (CNCTR).

➢ **Réunion du 1er décembre 2016**

• Audition de M. Jean-Jacques Urvoas, Garde des Sceaux, ministre de la Justice.

➢ **Réunion du 14 décembre 2016**

• Entretien avec deux membres du Comité parlementaire italien pour la sécurité de la République (COPASIR) : M. le sénateur Giacomo Stucchi (Président) et M. le sénateur Felice Casson (Secrétaire).

➢ **Réunion du 12 janvier 2017**

• Communication sur le rapport de la CVFS.

• Entretien avec M. Patrick Strzoda, directeur du cabinet de M. le Premier ministre.

➢ **Réunion du 22 février 2017**

• Entretien avec des membres du Comité du Parlement chargé de superviser les activités de renseignement et de sécurité du Royaume-Uni (« Intelligence and Security Committee ») : M. Dominic Grieve, président, membre de la chambre des Communes ; Lord Michael Lothian et Lord Robin Janvrin, membres de la chambre des Lords ; M. Keith Simpson, M. David Hanson et M. Richard Benyon, membres de la chambre des Communes.

Au total, au cours de l'année 2016 et au début de l'année 2017, la Délégation a tenu 20 réunions et elle s'est déplacée quatre fois ; l'ensemble de ces travaux représente une durée de près de 75 heures consacrées à l'information et au contrôle.

C. LE SUIVI DES RECOMMANDATIONS DE LA DPR FORMULÉES EN 2014 ET EN 2015

En 2014, la Délégation parlementaire au renseignement a émis 103 propositions, préparant ainsi la loi du 24 juillet 2015 ; en 2015, elle en a formulé 29.

Sur les 103 recommandations de 2014, les services du Coordonnateur national du renseignement indiquent un taux de prise en compte de 84,5 %.

De même, la majeure partie des recommandations de la DPR formulées en 2015 se sont trouvées prises en compte.

Cette attention soutenue du Gouvernement apportée aux observations de la Délégation est très satisfaisante.

Toutefois, en 2015, le rapport de la Délégation, présenté par M. Jean-Pierre Raffarin, avait insisté aussi sur l'importance de l'évaluation dans le domaine du renseignement – que celle-ci porte sur la politique conduite par les pouvoirs publics ou sur les services.

Or, sur ce dernier sujet, même si des progrès incontestables ont été réalisés en 2016, certaines avancées paraissent encore souhaitables.

Dans les pages qui suivent, nous donnerons l'exemple d'une proposition majeure de la DPR formulée en 2014 et qui a débouché en 2015 et en 2016 (la préfiguration du système PNR au niveau national) ; puis, nous réexaminerons la question de l'évaluation de la politique publique et des services de renseignement.

1. La préfiguration du système PNR à l'échelon national en attendant sa mise en place à l'échelle européenne

Le rapport de la DPR en 2014 avait proposé de mettre en place le système PNR à l'échelon national dans les plus brefs délais et de promouvoir également sa mise en œuvre à l'échelle européenne (proposition n° 1 du chapitre II).

En 2015 et en 2016, conformément aux souhaits de la Délégation, la préfiguration de la plateforme d'exploitation pour le système PNR au niveau national a été réalisée à l'aéroport de Roissy ; parallèlement, l'installation du système a débuté, de même que le raccordement d'un certain nombre de compagnies aériennes.

Nous apporterons, ci-dessous, quelques éléments d'information sur sa mise en place ; auparavant, nous rappellerons ce qu'est le PNR, tant national qu'européen, et nous donnerons quelques indications sur les négociations ayant permis de l'instaurer au niveau de l'Union européenne.

a. Le système PNR et les négociations européennes

Le PNR est l'acronyme de *« Passenger Name Record »* – ce qui signifie « *les données des dossiers passagers* », soit les données relatives aux passagers aériens pour les vols au départ ou à destination de la France (les vols intra-communautaires ne sont pas encore concernés).

Le PNR recouvre ainsi trois réalités :

– le PNR national, tout d'abord, qui ne concerne que les vols au départ ou à destination de la France (vols extra-communautaires). Plus de la moitié des États européens se sont, d'ores et déjà, dotés de PNR nationaux. Toutefois, ces fichiers ne sont pas interconnectés, ce qui limite leur efficacité face à des réseaux criminels transnationaux ;

– s'agissant des vols dans l'espace aérien européen, il est prévu, avec la directive européenne, que chaque État se dote d'un PNR national dont les caractéristiques seront harmonisées ;

– s'agissant enfin des vols transatlantiques, les États-Unis ont demandé, dans le courant de l'année 2011, que les Européens leur communiquent les données personnelles des passagers des vols concernés et qu'ils les intègrent dans leurs propres bases de données ; un accord a pu être trouvé sur ce point et le Parlement européen a ratifié l'accord PNR euro-américain en avril 2012.

À la suite de ce vote, les négociations sur le PNR européen ont débuté. Le Conseil a en effet demandé à la Commission de préparer un projet de PNR européen, sous la forme d'une directive.

Dans le courant de l'année 2015, la commission des libertés civiles du Parlement européen a adopté un premier texte.

Celui-ci était néanmoins difficilement applicable ; en particulier, la durée de conservation des données sur les passagers (identité, itinéraire, mode de paiement, etc.) et leur protection restaient autant de points qui n'avaient pas été tranchés.

Aussi les ministres de l'Intérieur, réunis le 20 novembre 2015 en séance extraordinaire à la demande du Gouvernement français, ont-ils demandé des progrès rapides sur le PNR.

L'accord finalement conclu entre les négociateurs du Parlement, ceux du Conseil et ceux de la Commission, le 2 décembre 2015, a permis de compléter utilement le texte.

Dans le cadre de cet accord, il a été arrêté que les données PNR fournies par les transporteurs aériens aux services de renseignements par les unités chargées de collecter les renseignements sur les passagers devaient être conservées par les transporteurs pendant une période de cinq ans.

Durant les six premiers mois, les données sont dites « non masquées », c'est-à-dire incluant les données d'identification personnelle.

Elles doivent ensuite être « masquées » pendant la période restante de quatre années et demie.

Les données « masquées » sont uniquement accessibles à un nombre limité de membres du personnel de l'unité de renseignements sur les passagers, ayant suivi une formation en matière de sécurité et faisant l'objet d'une habilitation.

Enfin, à l'issue de la période réglementaire de conservation, les données PNR devront être effacées de manière définitive, à moins que les États ne doivent les utiliser en raison d'enquêtes ou de poursuites pénales en cours.

Le texte de la directive a été adopté par la commission des libertés civiles du Parlement européen le 10 décembre 2015, puis par le Conseil le 21 avril 2016. Désormais, les États disposent d'un délai de deux ans pour transposer le dispositif définitif.

Il convient toutefois de relever que la directive connaît certaines limites. Par exemple, son périmètre ne concerne que la lutte contre le terrorisme et la criminalité grave. Il ne faut donc pas s'interdire de réfléchir à des améliorations éventuelles.

Proposition 1. La DPR souhaite que la transposition de la directive du 21 avril 2016 sur le PNR européen soit effectuée par les États membres le plus rapidement possible. Elle demande à la France d'accélérer cette transposition dans le droit national et à ses représentants auprès des différents gouvernements de l'Union européenne d'agir auprès d'eux pour qu'ils aillent dans le même sens. Elle note également que la directive présente certaines limites et elle suggère qu'une réflexion puisse être conduite pour renforcer encore l'efficacité du texte.

b. La préfiguration du système PNR à l'échelon national

La France avait fort heureusement, dès le mois de décembre 2010, pris la décision de se doter d'un système d'exploitation des données des passagers aériens.

Une mission interministérielle regroupant les ministères de l'Intérieur, de la Défense, des Transports et des Finances a été créée, dans le courant de l'année 2011, sous l'autorité du Premier ministre, pour mener les études de faisabilité, préparer les marchés, les lancer et en suivre l'exécution.

Le cadre juridique nécessaire au développement et à l'exploitation d'un tel système a été élaboré : l'article L. 232-7 du code de la sécurité intérieure, issu de la loi de programmation militaire du 18 décembre 2013 et complété par la loi du 28 juillet 2015 portant actualisation de cette programmation, définit les principes régissant le PNR. Les décrets du 26 septembre et du 22 décembre 2014 ont précisé les modalités pratiques de sa mise en œuvre, tandis que le décret du 21 octobre 2015 a prévu la mise en relation des données contenues dans le PNR avec celles figurant dans le fichier des personnes recherchées (FPR).

À l'issue des études de faisabilité, auxquelles les services de renseignement ont été étroitement associés, deux marchés ont été signés : le premier, à la fin de l'année 2013, pour l'assistance à la maîtrise d'ouvrage et le second, au début de l'année 2014, pour la réalisation du système lui-même.

La préfiguration de la plateforme d'exploitation du système, l'Unité information passagers (UIP), a été mise en place, à Roissy, dans des locaux dédiés, en septembre 2015.

Parallèlement, l'installation du PNR a débuté, de même que le raccordement d'un certain nombre de compagnies aériennes. Toutefois, le déploiement total du système ne sera pas achevé avant la fin de l'année 2017.

Actuellement, la mission PNR, en liaison avec l'UIP, prépare la mise à disposition effective du système à l'ensemble de ses futurs utilisateurs, notamment les services de renseignement, en vue de son exploitation opérationnelle.

2. L'évaluation de la politique publique du renseignement

Dans son rapport d'activité 2015, présenté par M. Jean-Pierre Raffarin, la DPR avait insisté sur l'évaluation de la politique publique du renseignement et également sur celle des services.

Le rapport de la DPR avait ainsi rappelé au Coordonnateur national du renseignement l'obligation législative d'établir un nouveau document d'évaluation, le rapport annuel d'activité des services de renseignement. Il avait également été préconisé d'améliorer la présentation du rapport annuel de synthèse des crédits consacrés au renseignement, prévu par la loi de programmation militaire 2014-2019. Enfin, une montée en puissance de l'ISR avait été souhaitée.

a. Le rapport annuel d'activité des services de renseignement et le rapport annuel de synthèse des crédits consacrés au renseignement

La proposition 28 du rapport de la DPR pour 2015 recommandait la création d'un rapport d'activité des services de renseignement publié par le Coordonnateur national du renseignement à la date n+1.

La proposition 24 avait aussi souhaité que la synthèse des crédits exécutés des services de renseignement – également présentée à l'année n+1 – soit coordonnée avec ce rapport d'activité.

Enfin, la proposition 25 demandait que des indicateurs de performance figurent dans le rapport de synthèse des crédits.

Le rapport annuel d'activité des services de renseignement et le rapport annuel de synthèse des crédits consacrés au renseignement ont été remis à la DPR le 3 novembre 2016 par le Coordonnateur national du renseignement. Ces deux documents concernent l'année 2015. Ils visent les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure et les services autorisés par le décret en Conseil d'État 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 dudit code.

Il s'agit là d'une avancée très importante qui doit permettre à l'ensemble des intervenants, et notamment au Parlement, de disposer d'une vision

approfondie des caractéristiques de la politique publique du renseignement et de l'activité des services au titre de l'année écoulée.

Pour autant, la communication de ces documents reste tardive.

La Délégation observe que le rapport annuel exhaustif des crédits consacrés au renseignement, qui porte sur l'exécution de l'année précédente, ne lui est transmis qu'à l'automne. Si la date de cette communication devait être maintenue, elle demande que ce document soit enrichi par des éléments sur l'exécution de l'année en cours et par une présentation des crédits pour l'année à venir.

Elle observe, en outre, qu'une communication en novembre du rapport annuel d'activité portant sur l'activité des services au cours de l'année précédente ne lui permet guère d'approfondir son travail en organisant des auditions particulières ou en se faisant communiquer des précisions par voie de questionnaires complémentaires. Elle souhaiterait donc que le rapport annuel d'activité lui soit présenté au cours du premier semestre de l'année.

Proposition 2. La DPR demande la remise du rapport annuel de synthèse des crédits de l'année précédente au plus tard le 1er avril de l'année en cours ; pour le cas où ce rapport ne pourrait être remis qu'à l'automne, elle demande que le document comporte également l'exécution des crédits de l'exercice en cours et une présentation des crédits inscrits dans le projet de loi de finances pour l'année à venir ; enfin, la DPR souhaite que le rapport annuel d'activité des services portant sur l'année précédente lui soit présenté avant le 30 juin de l'année en cours.

Par ailleurs, il convient de relever que les rapports présentés par le Coordonnateur national du renseignement comportent des indicateurs d'activité et des indicateurs de ressources.

Ces derniers correspondent à la présentation des crédits de paiement consacrés au financement des services de renseignement, des dépenses en fonds spéciaux par nature, des flux des ressources humaines, de l'effort de formation et de mobilité au sein des services, ainsi que des techniques de renseignement soumises à autorisation sur le territoire national.

Les indicateurs d'activité sont essentiellement quantitatifs et une réflexion est engagée, en lien avec le Coordonnateur national du renseignement, en vue d'affiner l'évaluation et de faire apparaître à l'avenir des critères qualitatifs.

En effet, ces indicateurs concernent trois fonctions majeures associées à l'activité des services de renseignement : l'aide à la décision, la prévention et la réduction des vulnérabilités, l'entrave et la neutralisation des menaces.

Dans le cadre de la fonction « aide à la décision », le Coordonnateur national du renseignement a élaboré un indicateur d'activité retraçant le nombre de notes destinées précisément à éclairer les responsables politiques. C'est ainsi que

l'on peut recenser 55 811 documents de ce type sur l'exercice 2015. Parmi eux, les 2/3 des documents (notes de renseignement, notes d'évaluation, dossiers thématiques) ont été réalisés par la DRM et la DGSE. Le ratio montre donc que ces deux services ont été particulièrement actifs en 2015, à la mesure du contexte et des enjeux opérationnels.

Au titre de l'activité « entrave et neutralisation des menaces », il existe aussi un indicateur qui dénombre les mesures administratives engagées par les différents services (perquisitions administratives, assignations à résidence, etc.). Le nombre total de ces mesures est de 583 en 2015. 61,8 % des actes administratifs ont été mis en œuvre par la DGSI dans le cadre, notamment, de la loi sur l'état d'urgence. Le ratio indiqué permet donc de bien saisir l'importance de l'activité de la DGSI dans le domaine de la lutte contre la menace terroriste.

b. La nécessaire montée en puissance de l'Inspection des services de renseignement

Le rapport de la DPR de 2015 avait aussi insisté, dans le cadre du dispositif général d'évaluation de la politique publique et des services de renseignement, sur l'importance de l'Inspection des services de renseignement.

Prévue par le Livre blanc sur la défense et la sécurité nationale de 2013, l'ISR a été créée par le décret n° 2014-833 du 24 juillet 2014.

Selon son article 2, l'ISR, placée sous l'autorité directe du Premier ministre, réalise « *des missions de contrôle, d'audit, d'étude, de conseil et d'évaluation à l'égard des services spécialisés de renseignement ainsi que de l'Académie du renseignement* ».

Ses membres sont désignés parmi les différents corps d'inspection des ministères concernés (Contrôle général des armées, Inspection générale de l'administration, Inspection générale des finances, Conseil général de l'économie, de l'industrie, de l'énergie et des technologies) par le Premier ministre, après avis du Coordonnateur national du renseignement, sur proposition de leurs ministres de tutelle. Ils continuent à exercer leurs attributions au sein de leurs corps d'appartenance respectifs.

Pour chaque mission, le Premier ministre désigne un chef de mission. Il fixe son mandat, ainsi que la composition de l'équipe devant l'assister. Le secrétariat de l'Inspection est assuré par le Coordonnateur national du renseignement.

La DPR, par application de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958, peut solliciter la communication de tout ou partie des rapports de l'Inspection. Ainsi, en 2015, deux rapports lui ont été transmis : le rapport visant à définir les contours du futur rapport d'activité des services de renseignement (« *Établissement d'un rapport d'activité des services de la communauté du renseignement* ») et le pré-rapport sur la mise en œuvre de la loi

de 2015 sur le renseignement. En 2016, la DPR a été destinataire du rapport final concernant la loi sur le renseignement (« *Mise en œuvre de la loi n° 2015-912 du 24 juillet 2015 en matière de techniques de recueil de renseignement* »).

Dans son rapport d'activité pour 2014, la DPR avait proposé que l'Inspection se dote d'un véritable chef de service afin qu'il incarne « *une certaine permanence en dépit de l'absence d'un corps d'inspection pérenne* » (proposition 6, page 72 du rapport de la Délégation).

Dans le courant de l'année 2016, un Secrétaire général de l'Inspection des services de renseignement a été désigné. On ne peut que se féliciter de cette décision, mais pour améliorer le suivi des travaux de l'ISR, il serait souhaitable de prévoir un renforcement du rôle et de l'autorité de son Secrétaire général.

Proposition 3. La DPR réitère sa demande de transformer le poste de Secrétaire général de l'ISR en un poste de chef de service, chargé de l'encadrement et du suivi des inspecteurs des services de renseignement.

Dans le cadre du plan de mission du Secrétaire général, pour l'année 2017 et éventuellement les années ultérieures, la DPR souhaiterait confier, sous couvert du Premier ministre, deux thèmes de réflexion à l'ISR. Naturellement, les résultats de ces études ne devraient pas être communiqués seulement à la DPR mais aussi aux principaux responsables de la politique publique du renseignement : le Président de la République, le Premier ministre et le Coordonnateur national. Le premier thème concerne les personnels des services de renseignement et le second les fichiers qu'ils utilisent.

Les demandes seront précisées dans la troisième partie du présent rapport qui présente les différents membres de la communauté du renseignement, ainsi que les préconisations de la Délégation en vue d'améliorer le fonctionnement de cette communauté sur certains points.

II. LA POLITIQUE DU RENSEIGNEMENT EN 2015 ET EN 2016

Deux missions ont particulièrement mobilisé les services en 2015 et en 2016 : la lutte antiterroriste et la lutte contre l'espionnage industriel, ainsi que contre les autres formes d'ingérence économique.

A. LA LUTTE ANTITERRORISTE

La sanctuarisation du territoire national face à la menace terroriste constitue aujourd'hui une priorité essentielle de la communauté du renseignement.

La mise en œuvre de cette priorité suppose une coordination forte entre les services. Telle est la raison pour laquelle celle-ci a été renforcée en 2014 et en 2015 – avec la création de la cellule HERMES (pilotée par la Direction du renseignement militaire), de la cellule INTERSERVICES (pilotée par la Direction générale de la sécurité intérieure) et de l'État-major opérationnel de prévention du terrorisme (EMOPT), placé directement auprès du ministre de l'Intérieur.

1. La politique générale du Gouvernement en matière de renseignement et la reconnaissance de la lutte antiterroriste comme objectif prioritaire

a. Le PNOR 2014-2019

Première étape du cycle du renseignement, le plan national d'orientation du renseignement (PNOR) est un document destiné à l'ensemble des services spécialisés de renseignement.

Ce document est élaboré par le Coordonnateur national du renseignement et il est approuvé par le Conseil national du renseignement, instance placée sous la présidence du Président de la République et devant laquelle le Coordonnateur exerce les fonctions de rapporteur ; par ailleurs, le Coordonnateur assure, en liaison avec le SGDSN, le secrétariat du CNR et il veille, également en liaison avec le SGDSN, à la mise en œuvre des décisions prises.

Le PNOR a pour but d'orienter l'action des services de renseignement, de déterminer leurs missions et leurs objectifs, et de les hiérarchiser.

Dans son édition 2014-2019, il définit sept axes d'efforts pour la protection des intérêts nationaux et trois axes d'efforts pour leur promotion. Pour chacun de ces axes, parmi lesquels la lutte antiterroriste, il détermine le ou les services en charge des différentes missions. Il arrête les objectifs qui leur sont assignés et il établit un ordre de priorité dans leur réalisation et dans les moyens à engager.

Le PNOR constitue ainsi la feuille de route stratégique des services. Il constitue aussi un instrument de coordination. Pour chaque axe d'efforts, le document désigne le ou les responsables et il organise leurs relations en vue de faciliter leurs interventions.

***

b. La progression des crédits et des effectifs des services de renseignement depuis 2013

DÉPENSES EN FONDS NORMAUX PAR SERVICES DE LA COMMUNAUTÉ DU RENSEIGNEMENT

(en millions d'euros)

	Exécuté 2013	Exécuté 2014	Exécuté 2015	Exécuté 2016	Dotation 2017
DGSE	641,24	654,81	672,50	711,63	669,82
DGSI	***	***	***	***	***
DRM	156,27	160,06	168,82	172,65	191,75
DRSD	96,48	95,06	98,32	105,61	119,08
DNRED	65,09	64,42	65,02	68,76	6,16 [(1)]
TRACFIN	7,14	7,44	10,26	13,66	14,90
Total Services spécialisés	*******	***	***	***	***
Académie du renseignement	1,08	1,30	1,20	1,25	1,41
CNR	0,57	0,71	0,65	0,65	0,67
Total Communauté	*******	*******	*******	*******	*******

[(1)] La dotation budgétaire de la DNRED pour l'exercice 2017 se lit hors crédits du titre 2.

Source : Coordination nationale du renseignement.

Les crédits de paiement consacrés au financement des services de la communauté du renseignement au sens strict (c'est-à-dire l'ensemble des services spécialisés de renseignement, l'Académie du renseignement et le Coordonnateur national du renseignement) ont connu une croissance très soutenue entre 2013 et 2016, passant de *** à *** milliard d'euros, soit une hausse globale de 11,3 %. Ces crédits regroupent les dotations relevant des différents programmes budgétaires de l'État consacrés à la politique du renseignement, hors fonds spéciaux.

Dans ce contexte, un effort tout particulier a été réalisé en faveur de la Direction générale de la sécurité intérieure (DGSI) ***. Les moyens alloués au service Tracfin ont également fortement progressé, passant de 7,14 millions d'euros en 2013 à 13,66 millions d'euros en 2016.

Les montants des crédits affectés à la Direction du renseignement militaire (DRM) et à la Direction générale de la sécurité extérieure (DGSE) ont également augmenté, respectivement de 10,48 % et de 10,97 %.

La Direction nationale du renseignement et des enquêtes douanières (DNRED) a vu ses moyens budgétaires progresser de 5,63 % sur la période.

NOMBRE D'AGENTS AU 31 DÉCEMBRE DE L'EXERCICE

	2013	2014	2015	2016
DGSE	5 094	5 154	5 257	5 376
DGSI	***	***	***	***
DRM	1 579	1 574	1 640	1 715
DRSD	1 052	1 076	1 147	1 190
DNRED	739	726	737	760
TRACFIN	92	104	119	132
Total Services spécialisés	***	***	***	***
Académie du renseignement	9	9	12	12
CNR	20	19	17	17
Total Communauté	***	***	***	***

Source : Coordination nationale du renseignement.

S'agissant des effectifs, le nombre des agents relevant de la communauté du renseignement au sens strict est passé, entre 2013 et 2016, de *** à *** (+ 10,45%).

Si, pour la seule période 2013-2015, on ajoute à ces personnels ceux du « second cercle », régis par l'article L. 811-4 du code de la sécurité intérieure, ainsi que ceux du Groupement interministériel de contrôle et ceux du Commissariat aux communications électroniques de défense (CCED), l'ensemble passe à *** en 2013 et à *** en 2015, soit une progression de + 8,3 %.

L'évolution des personnels a donc été plus rapide hors du premier cercle (+ 17,4 %) qu'en son sein (+ 5,7 %).

À l'intérieur de la communauté du renseignement, la croissance du nombre d'agents a été particulièrement notable pour la Direction générale de la sécurité intérieure et pour le service Tracfin.

En dehors de la communauté du renseignement, la croissance du nombre des agents participant à la politique publique du renseignement apparaît imputable principalement à l'Unité de coordination de la lutte antiterroriste (UCLAT), à la Direction centrale de la police judiciaire (DCPJ), au Service central du renseignement territorial (SCRT), à la Sous-direction de l'anticipation opérationnelle de la Gendarmerie nationale (SDAO) et à la Sous-direction de la sécurité intérieure (SDSI) de la Direction du renseignement de la Préfecture de police de Paris (DRPP).

Au total, il apparaît que cette évolution est parfaitement corrélée. Près de 80 % des moyens nouveaux sont affectés à la lutte antiterroriste.

L'accent a été mis en particulier sur les services du renseignement territorial qui avaient connu, de 2008 à 2013, une forte diminution de leurs effectifs, dans le cadre de la révision générale des politiques publiques (RGPP).

Proposition 4. Poursuivre, malgré les difficultés budgétaires, les recrutements au sein des services de renseignement, ainsi que le renforcement de leurs moyens matériels et humains.

2. La coordination interministérielle

Le dispositif de lutte antiterroriste repose sur l'efficacité et la performance des acteurs chargés de la coordination interministérielle. En effet, il est indispensable que l'information circule de manière fluide depuis les services de renseignement ou les groupes de travail interministériels vers les responsables politiques – et tout particulièrement vers les deux plus éminents d'entre eux : le Président de la République et le Premier ministre.

Il existe deux instances capitales en matière de coordination stratégique : le Coordonnateur national du renseignement, pour la coordination de l'action des services de renseignement, en prévention ou en entrave, et le SGDSN, pour la coordination interministérielle en matière de protection.

a. Le Coordonnateur national du renseignement

Depuis 2008, le Coordonnateur national du renseignement est chargé, en tout premier lieu, de la remontée du renseignement aux plus hautes instances de l'État.

Selon les dispositions de l'article R. 1122-8 du code de la défense, il conseille le Président de la République sur les questions de renseignement. Il l'informe, ainsi que le Premier ministre, par des points de situation quotidiens et par des synthèses de renseignement.

Il rapporte devant le Conseil national du renseignement, dont il prépare les réunions, et il veille à la mise en œuvre des décisions prises par le Conseil. Le SGDSN lui apporte son concours pour l'accomplissement de ses missions.

Il coordonne la communauté du renseignement. À ce titre, il coordonne l'action des services et hiérarchise leurs priorités, notamment à travers le PNOR.

Il réunit régulièrement les directeurs des services spécialisés de renseignement. Il favorise la mutualisation de leurs investissements. Il veille à la disponibilité des ressources budgétaires et des effectifs qui leur sont nécessaires. Il s'attache à la réalisation d'un environnement juridique bien adapté à leurs besoins.

Enfin, il pilote des fonctions transverses, notamment la formation – au travers de la présidence du Comité d'orientation et d'évaluation (COE) de l'Académie du renseignement – ou l'audit – où il joue un rôle moteur dans la définition du plan de charges de l'Inspection des services de renseignement.

Au total, le rôle du Coordonnateur national du renseignement est essentiel pour la coordination interministérielle des services de renseignement. En

particulier, son rôle est capital pour assurer une bonne remontée du renseignement auprès du Président de la République et du Premier ministre, et pour faciliter la prise de décision au plus haut niveau.

b. Le SGDSN

Aux termes du décret du 24 décembre 2009, le Secrétaire général de la défense et de la sécurité nationale assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Il anime et coordonne les travaux interministériels relatifs à la politique de défense et de sécurité nationale et aux politiques publiques qui y concourent.

Il élabore la planification interministérielle de défense et de sécurité nationale (comme Vigipirate) et coordonne la préparation des mesures de défense et de sécurité nationale incombant aux départements ministériels.

Il assure le secrétariat du Conseil de défense et de sécurité nationale.

Le Conseil national du renseignement étant une formation spécialisée du Conseil de défense et de sécurité nationale, le SGDSN apporte son concours au Coordonnateur national du renseignement, et il en assure le secrétariat.

Enfin, il assure, pour le Coordonnateur national du renseignement, le secrétariat de groupes de travail interministériels d'analyse et de synthèse sur les menaces, la prévention et la protection en matière de renseignement, dont les contributions sont destinées aux responsables politiques et aux responsables des services. Cette activité s'effectue sous le mandat du Coordonnateur, à la demande des plus hautes autorités de l'État et dans le respect du PNOR, afin de mieux cerner le champ du volet « protection » à mettre en œuvre.

Au total, il va sans dire que l'articulation entre les deux instances – la Coordination nationale du renseignement et le SGDSN – est une condition déterminante dans le pilotage de la politique publique du renseignement.

3. La coordination entre les services

Pour optimiser la performance de l'appareil de renseignement, il est apparu nécessaire de créer, au sein de certains départements ministériels, des centres de coordination destinés à améliorer la circulation de l'information au sein du département et destinés aussi à resserrer les liens avec d'autres services relevant d'autres ministères. Les cellules de coordination font ainsi figure d'organisations nodales – un partage du renseignement plus rapide, et multilatéral, permettant une meilleure communication et de meilleures synergies.

Le nombre de ces cellules a été significativement accru en 2015. Les attentats ont en effet incité l'État à renforcer son organisation et à accroître ses structures de coordination.

Quatre grandes structures de ce type sont en place : l'Unité de coordination de la lutte antiterroriste ; la cellule HERMES ; la cellule INTERSERVICES ; et enfin, l'État-major opérationnel de prévention du terrorisme.

Ces organismes permettent aux services de renseignement de nouer des dialogues à la fois fructueux et durables. Ces échanges sont essentiels pour orienter le recueil et l'intégration de renseignements issus de diverses origines et pour suivre les mouvements de personnes suspectes se déplaçant ou maintenant un contact entre les zones de combat du Moyen-Orient et le territoire national.

Par ailleurs, la mise en place de certaines de ces structures a nécessité une évolution rapide de la culture des différents services de renseignement – culture où le cloisonnement de l'information et les règles strictes de son partage étaient des principes solidement ancrés. C'est ainsi que les services ont pris l'habitude de participer à des dispositifs de mutualisation de l'information en temps réel, une évolution notable et positive qu'il convient de souligner.

a. L'UCLAT

L'Unité de coordination de la lutte antiterroriste a été créée en 1984 et elle est placée sous l'autorité du Directeur général de la police nationale.

L'UCLAT a pour mission de garantir la cohérence et l'efficacité du dispositif national de lutte contre le terrorisme.

À ce titre, l'UCLAT procède, pour le ministre de l'Intérieur, à l'actualisation permanente de la menace terroriste en réunissant des correspondants issus d'un certain nombre de départements ministériels (en particulier le ministère de la Défense), des représentants de la Coordination nationale du renseignement et des représentants du SGDSN.

L'UCLAT organise des réunions de coordination et de suivi pour la protection des personnes menacées, la sécurisation des grands événements, la surveillance des personnes ayant fait l'objet d'une interdiction judiciaire du territoire ou celle des personnes ayant fait l'objet d'une mesure administrative d'expulsion.

Elle est engagée dans la prévention de la radicalisation en assurant la gestion du Plan de prévention de la radicalisation et d'accompagnement des familles.

Elle participe à l'élaboration des plans de prévention et à la mise en œuvre des exercices de gestion de crise (en liaison avec le SGDSN).

Enfin, l'UCLAT peut demander, pour l'exercice de ses missions, la mise en œuvre d'une ou de plusieurs techniques de renseignement soumises à

autorisation sur le territoire national, telles qu'elles figurent dans la loi du 24 juillet 2015 relative au renseignement.

b. La cellule HERMES

Première cellule inter-agences, HERMES a été créée le 1er octobre 2014, sur proposition de la Direction du renseignement militaire. Sa mission est de coordonner et d'animer les échanges en matière de renseignement d'intérêt militaire, dans une logique d'appui à la planification et à la conduite des opérations.

À ce titre, la cellule HERMES regroupe les six services spécialisés de renseignement et le Commandement des opérations spéciales (COS). La DGSE contribue notamment à son fonctionnement en transmettant des données et en fournissant une expertise.

La cellule HERMES travaille également en relation étroite avec le Centre de planification et de conduite des opérations (CPCO).

Placée sous l'autorité du Directeur du renseignement militaire, la cellule HERMES joue désormais un rôle essentiel de conseil pour le chef d'état-major des armées et pour le ministre de la Défense. Elle constitue aussi un centre de renseignement indispensable pour les forces déployées sur les théâtres d'opérations extérieures.

c. La cellule INTERSERVICES

La cellule INTERSERVICES a été créée en juin 2015 à l'initiative de la DGSI. Elle a pour mission d'organiser la mise en commun des renseignements obtenus sur les organisations terroristes sunnites qui visent la France, et également d'accroître la capacité de réponse opérationnelle à cette menace.

Elle regroupe les six services spécialisés de renseignement, la Direction du renseignement de la préfecture de police de Paris et le Service central du renseignement territorial – auquel la Gendarmerie nationale est très étroitement associée. Le représentant du SCRT est, d'ailleurs, depuis juin 2015, un officier de gendarmerie.

La DGSI, en tant que chef de file en matière de lutte contre le terrorisme sur le territoire national, assure le pilotage de la cellule qui, hébergée par la DGSI, travaille au profit de tous les services qui la composent.

Cette cellule est ainsi devenue un point privilégié de partage de l'information opérationnelle sur les objectifs des services. Saisie par l'intermédiaire de chacun d'eux, elle a vocation à apporter son assistance aux enquêteurs, en mettant à profit les capacités des services partenaires dans une logique de complémentarité-subsidiarité.

La cellule fonctionne très bien car les participants disposent, par service, d'un terminal connecté au fichier central de leur organisme de rattachement ; il est ensuite facile de faire le point sur un dossier, en temps réel, de manière collective.

En complément de leur participation à la cellule INTERSERVICES, la Direction générale de la sécurité extérieure et la Direction générale de la sécurité intérieure ont mis en place, de manière bilatérale, une coopération renforcée et plus approfondie ; dans ce cadre, un groupe d'experts du Service du contre-terrorisme de la DGSE a été intégré à la Sous-direction de la lutte contre le terrorisme et les extrémismes violents de la DGSI.

d. L'EMOPT

L'État-major opérationnel de prévention du terrorisme a été créé le 9 juillet 2015. Il est placé directement sous l'autorité du ministre de l'Intérieur et il rassemble tous les services du ministère contribuant à la lutte contre le terrorisme.

L'EMOPT regroupe ainsi la DGSI, le Renseignement territorial, la police judiciaire, la Préfecture de police de Paris et la Gendarmerie. La coordination avec l'UCLAT se fait par le biais de la participation d'un membre de cette unité à l'État-major opérationnel.

L'EMOPT centralise la remontée des signaux faibles de tout le territoire – en particulier ceux qui ont été identifiés par le Service central du renseignement territorial et par la Sous-direction de l'anticipation opérationnelle de la Gendarmerie nationale. Il supervise ainsi l'action des préfets qui transmettent les informations concernant les personnes suspectes de radicalisation à partir des données recueillies localement par les services déconcentrés de l'État (ou par le numéro vert mis en place par l'UCLAT).

Il est également informé du traitement des dossiers les plus sensibles opéré par la DGSI.

L'UCLAT gère, en liaison avec l'EMOPT, un fichier de suivi de tous les signalements en matière de radicalisation et de terrorisme, et notamment des signalements obtenus au plus près du terrain. Il s'agit du fichier des signalés pour la prévention de la radicalisation à caractère terroriste (FSPRT).

B. LA LUTTE CONTRE L'ESPIONNAGE INDUSTRIEL ET CONTRE LES AUTRES FORMES D'INGÉRENCE ÉCONOMIQUE

Un autre pilier important de la politique publique du renseignement est la lutte contre l'espionnage industriel, ainsi que contre les autres formes d'ingérence économique.

1. L'espionnage industriel

L'espionnage industriel présente une menace grandissante, en raison notamment du durcissement de la concurrence internationale.

Plusieurs services spécialisés de renseignement participent, dans le cadre de leurs attributions, à la lutte contre l'espionnage industriel – espionnage qui porte principalement, outre les enjeux industriels, sur le volet technologique :

– le service Tracfin et la Direction nationale du renseignement et des enquêtes douanières y participent au titre du renseignement économique et financier (REF) ;

– la DGSE y participe au titre de son activité de surveillance à l'étranger, en mettant au jour des opérations d'espionnage susceptibles de capter tout ou partie du patrimoine économique et scientifique des entreprises ;

– enfin, la DGSI et la Direction du renseignement et de la sécurité de la défense sont plus particulièrement impliquées dans la lutte contre ce type d'ingérence. La DGSI dispose d'une sous-direction de *** qui veille à la protection du patrimoine économique de la Nation contre toute forme d'ingérence. La DRSD, pour sa part, dispose d'une division de la contre-ingérence économique au sein de la sous-direction de la contre-ingérence. Par ailleurs, elle participe à la protection des sites industriels de défense au moyen d'inspections de sécurité visant à détecter et à évaluer les vulnérabilités existantes et à faire des recommandations pour y remédier. Elle surveille aussi, avec l'appui et la coopération de la DGSI, les salons d'armement qui sont des lieux privilégiés pour l'espionnage industriel à caractère militaire.

2. Les autres formes d'ingérence économique

Cette mission recouvre la prévention, la détection, l'analyse, le signalement et l'empêchement de toutes situations, intentions ou actions – non nécessairement économiques – qui, légales ou non, sont susceptibles de nuire à un intérêt économique national, quel qu'il soit, au profit d'un intérêt étranger.

La protection du potentiel économique, scientifique et technique national, ainsi que la lutte contre les ingérences dont il peut faire l'objet, relève de la DGSI mais aussi de la DRSD, lorsque les intérêts liés à la défense nationale sont menacés.

Le service Tracfin surveille les mouvements de capitaux étrangers sur les comptes des établissements financiers nationaux. De son côté, la DRSD dispose d'une division de la contre-ingérence économique. Elle emploie aussi un bureau de la sécurité économique en lien avec la Direction générale de l'armement (DGA) et la Direction générale du Trésor, dans le cadre de la procédure de contrôle des investissements étrangers en France, lorsqu'il s'agit d'entreprises associées à l'effort industriel de défense.

Par ailleurs, au cours de l'été 2015, le Premier ministre a entrepris une réforme du dispositif français d'intelligence économique, débouchant sur un décret du 29 janvier 2016. Celui-ci institue, auprès du ministre chargé de l'Économie, un Commissaire à l'information stratégique et à la sécurité économiques.

Ce Commissaire est nommé par le Président de la République par décret en Conseil des ministres. Il dispose d'un service spécifique – le service de l'information stratégique et de la sécurité économiques – qu'il dirige, mais qui relève, pour son organisation et son fonctionnement, du ministère chargé de l'Économie. En pratique, une convention fixe les modalités de mise à disposition des moyens et des personnels.

Le Commissaire élabore et propose, en lien avec le SGDSN et avec les différents ministères concernés, la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation.

Les orientations en matière d'information stratégique et de sécurité économiques sont proposées au Premier ministre par un comité directeur composé de représentants ministériels et réuni à l'initiative du ministre chargé de l'Économie. Le Commissaire est chargé du secrétariat de ce comité.

Au total, le Commissaire et le service qu'il dirige ont pour vocation d'examiner toutes les questions qui concernent les atteintes aux intérêts fondamentaux de la Nation en matière économique, et de faire des propositions pour accroître la sécurité en ce domaine. Ils entretiennent un lien étroit avec les services de renseignement.

Les priorités actuelles du Commissaire à l'information stratégique et à la sécurité économiques sont les suivantes :

– l'établissement d'une cartographie de toutes les entreprises d'intérêt national en matière économique, industrielle ou scientifique ;

– le développement de standards de conformité, c'est-à-dire la définition de comportements-types que les entreprises devraient adopter dans leurs relations financières avec l'étranger, afin d'éviter qu'elles ne se trouvent confrontées – à la faveur d'opérations commerciales internationales et souvent à leur insu – à des situations de blanchiment financier, de corruption ou d'ingérence ;

– la définition de stratégies et de règles juridiques en matière de normalisation ;

– la définition de stratégies et de directives en matière de défense de la souveraineté numérique.

Par ailleurs, le Commissaire et le service de l'information stratégique et de la sécurité économiques réunissent tous les mois le CORIE – le comité du

renseignement d'intérêt économique – où siègent *** Ils peuvent ainsi faire le point, de manière régulière, sur toutes les actions d'ingérence économique qui sont identifiées au sein de ce comité.

Au-delà de ces tâches très importantes, il serait intéressant que le champ de compétence du Commissaire à l'information stratégique et à la sécurité économiques puisse être élargi à de nouvelles missions :

– une structure de pilotage dans le domaine des standards de conformité s'appliquant aux entreprises qui commercent avec l'étranger doit être créée. Aujourd'hui, en effet, les entreprises qui ont des relations commerciales internationales ne trouvent pas toujours les réponses nécessaires lorsqu'elles s'interrogent sur l'honorabilité réelle de leurs cocontractants. Un correspondant dédié doit pouvoir les éclairer à cette fin, indépendamment du service de l'information stratégique et de la sécurité économiques ;

Proposition 5. Il serait souhaitable que le Commissaire à l'information stratégique et à la sécurité économiques puisse définir les bases juridiques nécessaires à la création d'une organisation référente en matière de conformité anti-corruption ; cette structure servirait de conseil aux entreprises entretenant des relations commerciales soutenues avec l'étranger.

– en second lieu, il serait d'un grand intérêt que le Commissaire à l'information stratégique et à la sécurité économiques conduise des études concernant les objets connectés. Ceux-ci, en effet, vont se développer de manière considérable dans les dix prochaines années. Il ne faudrait pas en arriver à une situation où l'industrie française serait totalement dépendante de ces objets – notamment en tant que composants pour d'autres technologies – ou encore à une situation où les entreprises seraient contraintes de recourir à certains d'entre eux – alors qu'ils pourraient comporter des failles sciemment mises en place par des puissances ou des entreprises étrangères.

Proposition 6. Intégrer dans les études conduites par le Commissaire à l'information stratégique et à la sécurité économiques la question des objets connectés, afin qu'il prépare une réglementation propre à ces objets.

III. LES PROBLÈMES RENCONTRÉS PAR LA COMMUNAUTÉ DU RENSEIGNEMENT EN 2015 ET EN 2016, ET LES PRÉCONISATIONS DE LA DÉLÉGATION

La politique publique du renseignement est, en tout premier lieu, confiée aux services spécialisés de renseignement. Ceux-ci, aux termes des dispositions du décret n° 2014-474 du 12 mai 2014 pris pour l'application de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et portant désignation des services spécialisés de renseignement, sont au nombre de six et ils forment « le premier cercle ». Ils recourent de manière constante aux techniques de renseignement soumises à autorisation sur le territoire national en vertu de la loi du 24 juillet 2015 relative au renseignement.

Cependant, ces six services ne sont pas les seules administrations qui opèrent dans le domaine du renseignement. Il convient de distinguer aussi les services dits du « second cercle », organismes mentionnés par l'article L. 811-4 du code de la sécurité intérieure. Aux termes du décret n° 2015-1639 du 11 décembre 2015 pris pour l'application de cet article, ces services relèvent de la Direction générale de la Police nationale (DGPN), de la Direction générale de la Gendarmerie nationale (DGGN) et de la Préfecture de Police de Paris. Ces services ont également la possibilité de recourir à des techniques de renseignement soumises à autorisation sur le territoire national en vertu de la loi du 24 juillet 2015, dans le périmètre précis de leurs missions.

Enfin, il existe quelques services de renseignement à statut spécifique. Ils ne ressortissent ni du décret du 12 mai 2014, ni de celui du 11 décembre 2015, et ils n'ont pas accès aux techniques de renseignement prévues par la loi du 24 juillet 2015. Dans cette dernière catégorie, on peut citer le service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée (SIRASCO) qui relève du ministère de l'Intérieur ou encore le bureau du renseignement pénitentiaire, relevant du ministère de la Justice [(1)].

Dans une première partie, seront passés en revue un certain nombre de services de renseignement, membres des différents cercles de la communauté, et quelques recommandations effectuées pour résoudre certaines de leurs difficultés ponctuelles.

Puis, dans une deuxième partie, seront examinées trois questions concernant l'ensemble des acteurs du renseignement.

---

(1) Toutefois, 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 a 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. Le projet de décret en Conseil d'État nécessaire à la mise en œuvre de la loi sera adopté très prochainement. Il a été présenté dans ses grandes lignes par M. Jean-Jacques Urvoas, ministre de la Justice, Garde des Sceaux, lors de son audition par la Délégation le 1er décembre 2016.

Enfin, dans une troisième partie, nous verrons qu'il ne paraît pas utile, dans l'immédiat, d'accroître le nombre des organismes de coordination institutionnelle.

A. LA COMMUNAUTÉ DES ACTEURS DU RENSEIGNEMENT

1. Les six services spécialisés de renseignement

Seront passés en revue successivement la Direction générale de la sécurité extérieure, la Direction générale de la sécurité intérieure, la Direction du renseignement militaire, la Direction du renseignement et de la sécurité de la défense, la Direction nationale du renseignement et des enquêtes douanières, et enfin, le service Tracfin.

a. La Direction générale de la sécurité extérieure

Créée par le décret n° 82-306 du 2 avril 1982, la DGSE, service de renseignement extérieur, a pour mission, de *« rechercher et d'exploiter les renseignements intéressant la sécurité de la France, ainsi que de détecter et d'entraver, hors du territoire national, les activités d'espionnage dirigées contre les intérêts français afin d'en prévenir les conséquences »*.

Rattachée au ministère de la Défense, la DGSE est le service de renseignement extérieur de la France, avec une double mission de renseignement et d'action. La DGSE détient le monopole de l'action clandestine à l'étranger. De plus, elle dispose d'une capacité d'intervention clandestine pour *« effectuer, dans le cadre de ses attributions, toute action qui lui serait confiée par le Gouvernement »*.

Cette disposition fait de la DGSE non seulement un service secret mais aussi un service spécial. Historiquement, d'ailleurs, le « service action » a été constitué, à la Libération, en prélevant sur les effectifs du 11e Choc qui était un bataillon de parachutistes et de commandos.

Fin 2015, les effectifs de la DGSE, ***, s'élevaient à 6 315 agents. Ils ont été portés à 6 463 fin 2016.

Il convient de noter que les effectifs de la DGSE progressent de manière constante depuis 2008. En effet, dans le cadre de la loi de programmation militaire 2008-2013, on relève la création nette de 616 emplois ; puis, sur la période 2014-2019, on enregistre à nouveau la création de 797 emplois. En 2019, il est ainsi prévu que les effectifs de la DGSE atteignent environ 6 000 ETPT (hors service action).

Ces 797 emplois sont ventilés de la manière suivante :

– 281 emplois au titre de la loi de programmation militaire initiale ;

– 185 emplois au titre d'une décision du Premier ministre à la suite des attentats du mois de janvier 2015 ;

– 140 emplois dans le cadre de l'actualisation de la loi de programmation militaire en juillet 2015 ;

– 191 emplois à la suite d'un arbitrage interministériel suites aux attentats de novembre 2015.

Par ailleurs, sur ces 797 créations d'emplois, 287 créations ont été effectivement budgétées au cours de la période 2014-2016 (soit 59 créations en 2014, 106 en 2015 et 122 en 2016). Le solde (510 créations d'emplois) devrait s'échelonner jusqu'en 2019, à raison de 124 créations en 2017, 189 créations en 2018 et 197 créations en 2019.

La répartition catégorielle de ces créations d'emplois montre qu'il s'agit, pour les trois-quarts, de personnels de catégorie A et d'officiers. Pour un quart, de personnels de catégorie B et de sous-officiers. En revanche, les personnels administratifs de catégorie C diminuent.

Une évolution des infrastructures immobilières est nécessaire pour accueillir ces personnels supplémentaires.

Dans l'immédiat, la DGSE a arrêté un programme pluriannuel de rénovation immobilière qui s'élève à un peu moins de 160 millions d'euros sur la période 2015-2017 – soit 52 millions d'euros pour l'année 2015, 20,54 millions d'euros pour l'année 2016 (27,5 millions d'euros si l'on inclut la location des structures temporaires utilisées pendant la durée des chantiers) et 75 millions d'euros pour l'année 2017. Ce plan concerne les trois implantations de la DGSE à Paris et en proche banlieue.

Ensuite, l'ensemble des opérations programmées sera intégré dans un schéma directeur immobilier se déroulant sur 10 ans – en l'occurrence sur la période 2016-2025. Ce schéma sera finalisé d'ici la fin du second semestre de l'année 2017, afin de faire face, d'une part, au fort besoin d'entretien du patrimoine existant et, d'autre part, à la forte augmentation de ses ressources humaines. Il sera nécessaire d'examiner les besoins budgétaires complémentaires pour la réalisation de ce schéma directeur.

Dans le cadre de la préparation de ce schéma directeur immobilier, et indépendamment des travaux de rénovation et de mise en sécurité, compte tenu de l'arrivée à saturation des sites de la DGSE dans le contexte de poursuite de sa montée en puissance, il pourrait être intéressant que la DGSE étudie, en liaison avec le ministère de la Défense, la possibilité d'acheter ou de faire construire des

locaux supplémentaires afin d'accueillir ses nouveaux effectifs, tout en menant les travaux de rénovation et de mise en sécurité indispensable.

b. La Direction générale de la sécurité intérieure

La Direction générale de la sécurité intérieure a été créée par le décret n° 2014-445 du 30 avril 2014. Elle reprend les missions de la Direction centrale du renseignement intérieur (DCRI), créée en 2008, elle-même issue de la fusion de la Direction centrale des renseignements généraux (DCRG), née en 1907, et de la Direction de la surveillance du territoire (DST), créée en 1944.

La DGSI est compétente en matière de contre-espionnage, de lutte contre le terrorisme, de lutte contre les extrémismes ou les séparatismes violents (comme en Corse ou au Pays basque), de lutte contre la prolifération des armes de destruction massive, de lutte contre la criminalité liée aux technologies de l'information et de la communication, et de contre-ingérence criminelle ; elle contribue à la surveillance des communications électroniques et radioélectriques.

La DGSI dispose d'un maillage territorial important. Elle est également dotée de *** postes à l'étranger distincts du réseau de la Direction de la coopération internationale de la Direction générale de la police nationale.

À Paris et en région parisienne, la DGSI est renforcée par la Direction du renseignement de la préfecture de police de Paris – en application du décret du 30 avril 2014 qui précise que *« le service chargé, sous l'autorité du Préfet de police, de missions de renseignement intérieur concourt à l'activité de la DGSI qui peut se saisir, concurremment avec lui ou de manière exclusive, de toute question traitée par ce service »*. Toutefois, la DGSI reste seule compétente pour toutes les enquêtes qui concernent le contre-espionnage, la contre-prolifération et la sécurité économique.

De 2015 à 2016, les effectifs de la DGSI ont été augmentés de plus de *** postes. Cette hausse s'inscrit dans le cadre de trois plans de renforcement cumulés (le plan Livre blanc de 2013, le plan de lutte anti-terroriste de 2015 et le pacte de sécurité).

Cette hausse des effectifs pose actuellement deux problèmes à la DGSI :

– tout d'abord, il faut parvenir à réaliser tous les recrutements correspondant aux créations de postes ; et, en particulier, il faut parvenir à recruter tous les personnels d'ingénierie qui sont nécessaires à la DGSI – les recrutements s'effectuant dans un contexte de forte concurrence pour des ressources humaines rares ;

– ensuite, se pose la question des locaux pour accueillir ces personnels ; en effet, les implantations existantes de la DGSI trouvent leurs limites pour accueillir un millier d'agents supplémentaires à l'horizon 2018.

Il faut donc que la Direction de l'immobilier de l'État – service qui dépend de la Direction générale des finances publiques et qui exerce le suivi des demandes des administrations lorsqu'elles souhaitent faire des acquisitions immobilières – trouve, en liaison avec le ministère de l'Intérieur, une implantation unique et bien adaptée pour la DGSI.

Enfin, la DPR estime que la répartition géographique des personnels recrutés devra bénéficier aussi aux échelons départementaux et régionaux de la DGSI.

En effet, c'est au niveau départemental et régional que s'effectuent les échanges avec les autres services déconcentrés de l'État, notamment en ce qui concerne la détection et l'analyse des signaux faibles.

En pratique, ces échanges se déroulent au sein de « groupes d'évaluation » rassemblant, chaque semaine, sous l'autorité du préfet, les représentants départementaux des services compétents, dont la DGSI, le SCRT et la Gendarmerie nationale. Ce sont les « réunions de l'État-major de sécurité ». Dans ce cadre, les signaux faibles issus des territoires sont étudiés et sont évalués. Puis, à partir de l'évaluation, les dossiers sont confiés au partenaire compétent – et notamment à la DGSI, lorsque les signalements relèvent du terrorisme et non d'un simple processus – fût-il caractérisé – de radicalisation.

Ainsi, dans l'intérêt de la coordination entre ces services et du traitement des signaux faibles, les fonctionnaires de la DGSI doivent être en nombre suffisant dans les départements et dans les régions.

Proposition 7. Réfléchir à une nouvelle implantation mieux adaptée pour le siège de la DGSI et accélérer les recrutements au sein des échelons départementaux et régionaux de ce service.

c. La Direction du renseignement militaire

La DRM, service de renseignement des armées, a été créée en 1992. Ses missions sont définies par l'article D. 3126-10 du code de la défense.

Il est précisé aux termes de cet article, que la DRM *« relève du chef d'état-major des armées dont elle satisfait les besoins en renseignement d'intérêt militaire »*. Par ailleurs, le directeur du renseignement militaire *« assiste et conseille le ministre de la défense en matière de renseignement d'intérêt militaire »*.

Le rôle de la DRM est donc, à la fois, de garantir aux autorités politiques et aux responsables militaires une autonomie d'appréciation des situations au niveau stratégique et de fournir aux forces engagées en opération le renseignement nécessaire à la planification et à la conduite de la manœuvre au niveau tactique.

Les arrêtés du 30 et du 31 mars 2016 précisent l'organisation et les attributions de la DRM. Il est notamment indiqué dans ces textes que la DRM

exerce la responsabilité de pilotage de la fonction interarmées du renseignement. À ce titre, elle coordonne l'ensemble des organismes des armées qui contribuent à la recherche et à l'exploitation du renseignement, soit environ 8 000 personnes.

Pour remplir ses missions, la DRM dispose d'un panel complet de capteurs (renseignement d'origine image, électromagnétique, cybernétique et humain) qui relèvent de ses moyens propres et de ceux des armées déployés sur les théâtres d'opérations.

Les effectifs de la DRM ont augmenté au cours de l'année écoulée, passant de 1 640 agents en 2015 à 1 715 en 2016. Dans le cadre de l'actualisation de la loi de programmation militaire 2014-2019, ils devraient atteindre 2 100 personnes en 2019. La DRM recrute à la fois des militaires et des personnels civils ; ces derniers représentent 26 % du personnel en 2016 ; leur effectif devrait atteindre 30 % en 2019.

Face aux données de masse produites par les nouvelles capacités spatiales (programmes CERES et MUSIS) et numériques (au sein du cyberespace), les effectifs de la DRM restent limités. L'enjeu dans le domaine des ressources humaines, pour les années à venir, sera donc de pouvoir disposer d'un vivier suffisamment large au sein des armées et d'une capacité de rémunération du personnel civil suffisamment compétitive pour recruter du personnel adapté aux défis du renseignement d'intérêt militaire.

Afin de relever les défis techniques auxquels elle se trouve confrontée, en particulier dans le domaine de l'imagerie et du renseignement géo-spatial, la DRM a décidé de créer, sur sa base de Creil, un pôle de compétitivité dédié au renseignement d'intérêt militaire. Il regroupera des entreprises (grands groupes, PME et start-up), ainsi que des organismes de recherche et de formation. Les premières entités doivent s'installer dès le début de l'année 2017.

d. La Direction du renseignement et de la sécurité de la défense

Aux termes de l'article D. 3126-5 du code de la défense, la Direction du renseignement et de la sécurité de la défense est le service *« dont dispose le ministre de la défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles »*.

La dénomination de « Direction du renseignement et de la sécurité de la défense » s'est substituée à celle de « Direction de la protection et de la sécurité de la défense » par application des dispositions du décret n° 2016-1337 du 7 octobre 2016.

Cette dénomination clarifie la mission de cette Direction dont le renseignement de contre-ingérence a toujours été le cœur de métier. L'évolution de cette mission, qui est concomitante à l'évolution de la menace, se manifeste par la part croissante accordée aux métiers liés à la recherche et à l'analyse, ainsi qu'aux métiers liés à l'informatique et à la cyberdéfense.

Les caractéristiques principales des attributions et des actions conduites par la DRSD sont les suivantes :

– la DRSD apporte son concours aux différents échelons de commandement pour l'exercice de leurs responsabilités en matière de sécurité ; de plus, elle est reconnue par l'OTAN comme agence nationale de contre-ingérence militaire ;

– la DRSD agit essentiellement dans un cadre préventif ; son engagement recouvre deux types d'actions permanentes et complémentaires : l'acquisition du renseignement de contre-ingérence et le contrôle des mesures de protection de la sphère « défense » ;

– l'action de la DRSD s'étend sur l'ensemble des menaces du spectre dit « TESSCo » (pour terrorisme, espionnage, sabotage, subversion et crime organisé), lorsque ces menaces concernent la sphère de défense ; cette sphère comprend, d'une part, l'ensemble des ressortissants de la défense – c'est-à-dire les forces armées, les administrations centrales et les services liés à la défense (à l'exception de la DGSE) – et, d'autre part, l'ensemble du secteur économique en rapport avec la « mission défense » – ce qui inclue notamment la base industrielle et technologique de défense (BITD), ainsi que les acteurs économiques ou institutionnels qui opèrent sur les programmes d'armement, les technologies duales, la recherche et le développement, ou le soutien aux exportations ;

– la DRSD suit ainsi près de *** sociétés en lien contractuel avec la défense, auxquelles s'ajoutent celles qui, sans être en lien, présentent un intérêt fort dans le domaine de la défense en raison de leur secteur d'activité ; dans l'environnement de ces sociétés, les actes d'espionnage ou criminels par voie cybernétique, ou encore l'instrumentalisation du droit à des fins de prédation économique, sont des pratiques fréquentes ; ces modes opératoires – qui visent à capter directement des savoir-faire et des technologies ou à éliminer la concurrence en déstabilisant financièrement des entreprises – menacent le potentiel industriel et scientifique de la défense et, par voie de conséquence, les intérêts fondamentaux de la Nation ;

– dans le cadre de sa mission de contre-ingérence, la DRSD contribue directement, en liaison avec la Direction générale de l'armement, à la politique de protection du potentiel scientifique et technique de la nation (PPSTN), lorsque ce dernier intéresse la défense ; cette action s'inscrit dans un cadre interministériel et suppose une coordination avec le SGDSN et avec le Service de l'information stratégique et de la sécurité économique (SISSE) ;

– cette action de la DRSD s'étend également au cyberespace – ce qui passe, par exemple, par l'homologation, en liaison avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), des dispositifs de sécurité informatique des industries de défense.

S'agissant des personnels, des mesures successives ont été prises pour accroître, de manière significative, le dimensionnement des moyens. Les missions de la DRSD – dont la lutte antiterroriste, la protection du potentiel scientifique et technique de la Nation (PPST) et les actions préventives – impliquent en effet un format de ressources humaines approprié.

La loi de programmation militaire 2014-2019 a prévu le renforcement de la DRSD qui comptait 1 500 personnes en 2008, mais dont les effectifs avaient été ramenés à 1 052 personnes à la fin de l'année 2013. Cette remontée en puissance, amorcée en 2014, a connu une accélération dans le cadre de la lutte antiterroriste et de l'actualisation de la loi de programmation militaire de juillet 2015. Pour la fin de l'année 2016, l'effectif cible est ainsi passé à 1 190 personnes. Il devrait être de 1 307 personnes pour 2017 et de 1 543 personnes pour 2019.

L'organisation de la direction centrale a été ajustée pour intégrer le retour d'expérience des événements de janvier 2015 et pour prendre en compte la loi du 24 juillet 2015 relative au renseignement. Les renforts alloués par le Gouvernement au titre de la lutte antiterroriste (45 en 2015, 20 en 2016) ont permis les ajustements organisationnels d'urgence nécessaires pour consolider la capacité de réponse opérationnelle du service dans le contexte des menaces pesant actuellement sur la sécurité de la défense.

Dans ce cadre, plusieurs actions ont été menées telles que la création du centre de suivi des opérations (CSO) et celle d'une plateforme intégrée antiterroriste (PIAT). Ces dernières sont à associer à la montée en puissance des moyens techniques de recueil du renseignement et à la participation active aux structures interministérielles d'antiterrorisme. En apportant une puissance de travail supplémentaire, davantage de réactivité et une plus grande adaptabilité, ces actions menées par la DRSD ont démontré toute leur pertinence en novembre 2015 puis en juillet 2016.

Pour autant, la démarche de recrutement est complexe. En effet, la remontée des effectifs militaires de la DRSD, comme pour la DRM, est ardue du fait de sa dépendance à l'égard des directions des ressources humaines des armées, confrontées elles-mêmes à un besoin urgent de recrutement. Par ailleurs, l'objectif d'augmentation du ratio civils / militaires se heurte aux conditions financières de recrutement de spécialistes de haut niveau dans un contexte de forte concurrence concernant les spécialités considérées comme critiques (SIC [1] et Cyber notamment). Toutefois, la DRSD s'est engagée dans une politique de rééquilibrage entre personnels militaires et personnels civils. La part de ces derniers devrait ainsi passer de 21 à 25 % de 2014 à 2019.

Enfin, la DRSD participe à tous les grands dispositifs de coordination qui existent entre les services :

(1) Système d'Information et de Commandement.

– elle est membre de la cellule HERMES, créée en octobre 2014 à l'initiative de la DRM et placée près du CPCO pour échanger le renseignement utile à la planification et à la conduite des opérations militaires ;

– dans le domaine de la lutte antiterroriste sur le territoire national, elle a pour partenaire privilégié la DGSI ; la collaboration avec la DGSI a encore été renforcée avec la création, en 2015, de la cellule INTERSERVICES ;

– elle collabore avec la DGSE sur des questions portant principalement sur la protection des forces françaises déployées à l'extérieur ;

– elle participe à des réunions avec la DRPP, avec le Bureau du renseignement pénitentiaire et avec les préfets de zone.

e. La Direction nationale du renseignement et des enquêtes douanières

La Direction nationale du renseignement et des enquêtes douanières a été créée dans sa forme actuelle par un arrêté du 29 octobre 2007 et a été placée sous l'autorité de la Direction générale des douanes et des droits indirects (DGDDI).

Elle lutte contre la contrebande et la fraude organisée en conduisant des opérations destinées à saisir des marchandises et des sommes d'argent et en identifiant des filières en vue de leur démantèlement. Elle a ainsi pour mission de collecter des renseignements à caractère commercial, économique et financier, et portant sur les fraudes en général. Sur cette base, elle est amenée à orienter, voire à encadrer, le travail des services déconcentrés de la DGDDI, en particulier celui de la brigade des douanes. Cette approche, très globale, des circuits et des vecteurs de la grande fraude lui permet de s'engager fortement dans la lutte contre les différents trafics, notamment les trafics de produits stupéfiants, de produits contrefaits, de tabac et d'armes. Enfin, la DNRED participe également à la lutte contre le terrorisme et au démantèlement des circuits financiers qui l'alimentent. Le nombre d'agents de la DNRED est resté stable de 2013 à 2016. Au 31 décembre 2016, il s'élève à 760 personnes.

f. Le service Tracfin

Institué par décret du 9 mai 1990 portant création d'une cellule de coordination chargée du traitement du renseignement et de l'action contre les circuits financiers clandestins, le service Tracfin participe à la protection de l'économie nationale et a pour mission de lutter contre les circuits financiers clandestins, le blanchiment de capitaux et le financement du terrorisme.

Érigé en service à compétence nationale depuis le 6 décembre 2006, et placé sous la tutelle du ministre chargé de l'Économie et des finances, Tracfin répond à la dénomination de cellule de renseignement financier nationale, à la fois au sens du Groupe d'action financière (GAFI) et de l'Union européenne, à savoir une « *cellule nationale centrale chargée de recevoir et, dans la mesure de ses pouvoirs, de demander, d'analyser et de communiquer aux autorités compétentes*

les informations divulguées concernant un éventuel blanchiment de capitaux, un éventuel financement du terrorisme ou toute information requise par les dispositions législatives ou réglementaires nationales ».

Le service est composé de deux départements opérationnels : le département de l'analyse, du renseignement et de l'information et le département des enquêtes ; d'un département des affaires administratives et financières ; d'une division en charge de la lutte contre le financement du terrorisme ; d'une mission des systèmes d'information ; et d'un pôle juridique et judiciaire. La progression des effectifs a été continue et particulièrement forte ces dernières années. Le service est passé de 72 agents en 2010 à 132 agents en 2016, dont six agents de liaison mis à disposition de Tracfin par leur administration d'origine.

Tracfin est une structure opérationnelle, destinataire unique et exclusif des déclarations de soupçon susceptibles de concerner le blanchiment du produit d'infractions passibles de plus d'un an d'emprisonnement, les fraudes aux finances publiques ou le financement du terrorisme. Ces déclarations émanent aujourd'hui de plus de 40 professions assujetties au dispositif de lutte anti-blanchiment, soit près de 200 000 professionnels sur le territoire national.

À partir de ces déclarations de soupçons et des informations reçues de ses homologues étrangers, d'autres administrations de l'État, ou encore des autorités de contrôle des professionnels assujettis, Tracfin a pour mission de recueillir, d'analyser, d'enrichir et d'exploiter tout renseignement propre à établir l'origine ou la destination délictueuse d'une opération financière. Seules ces catégories d'information permettent à Tracfin d'entreprendre des investigations ; la loi exclut toute possibilité pour le service de se saisir sur le fondement de révélations autres, notamment les dénonciations anonymes et celles effectuées par les particuliers ou par voie de presse. Le dispositif contribue à fiabiliser l'origine de l'information et justifie la protection de la source.

Les déclarations de soupçon ou les informations reçues sont tout d'abord intégrées dans la base de données du service et rapprochées avec d'éventuelles données préexistantes. Tracfin conserve les informations reçues pendant 10 ans, délai prorogé de 10 ans en cas de transmission à l'autorité judiciaire.

Si les informations reçues sont exploitables, les agents du service les rapprochent de toute information utile recueillie dans les fichiers administratifs auxquels ils ont accès, directement ou indirectement, ou auprès des administrations partenaires (police judiciaire, douane, services de renseignement, administration fiscale, organismes sociaux, etc.). Les bases ouvertes sont aussi exploitées.

Au besoin, des cellules de renseignement financier étrangères peuvent être interrogées quand des liens financiers, voire juridiques (par exemple, domiciliation de sociétés), sont mis en évidence.

Enfin, les agents recueillent et analysent, par l'exercice du droit de communication, tout document utile auprès des professionnels assujettis (relevés de comptes, actes notariés, statuts de société, documents d'expertise comptable, factures, documents d'ouverture de comptes, etc.) ou de toute administration ou personne chargée d'une mission de service public, telles les institutions financières et l'administration fiscale. Le service dispose également du pouvoir de s'opposer à l'exécution d'une opération qui lui est signalée et de la suspendre pendant un délai de 10 jours ouvrables, avant que les autorités judiciaires ne prennent le relais et effectuent, le cas échéant, des saisies pénales.

La divulgation des informations que détient Tracfin est encadrée par le code monétaire et financier qui assigne à Tracfin une finalité judiciaire. En effet, si, à l'issue de ses investigations, le service met en évidence des faits susceptibles de relever du blanchiment d'une infraction punie d'une peine privative de liberté supérieure à un an ou du financement du terrorisme, la loi prévoit que Tracfin doit saisir le procureur de la République territorialement compétent par note d'information.

Parallèlement à cette obligation pour Tracfin de saisir les autorités judiciaires en cas de présomption d'infraction pénale, le service peut décider d'externaliser ses informations à d'autres destinataires visés par le code monétaire et financier et notamment aux autres services de renseignement de la communauté.

Tracfin a connu une forte progression de son volume d'activité en 2015 tant par le nombre d'informations reçues que par le nombre d'informations externalisées. Le service a reçu 45 266 informations (+18 % par rapport à 2014) dont 43 231 déclarations de soupçon émanant des professionnels déclarants. Sur cette même période, le service a réalisé 10 556 enquêtes, soit une hausse de 8 % par rapport à 2014.

Service de renseignement financier et membre du Conseil national du renseignement depuis 2008, la coopération de Tracfin avec les partenaires du « premier cercle » de la communauté du renseignement se traduit notamment par une participation aux cellules INTERSERVICES et HERMES. En particulier, un agent de Tracfin est présent au sein de la cellule INTERSERVICES avec un accès sécurisé au système d'information de Tracfin pour effectuer des criblages en temps réel depuis le mois de juin 2016. Sur la base des déclarations de soupçon adressées par les professionnels et prévues par le code monétaire et financier, Tracfin effectue des demandes de criblage auprès des différents services du « premier cercle » afin d'établir des liens avec des informations détenues par ces services et engager des investigations. La coopération prend également la forme de transmissions spontanées de Tracfin qui, après enrichissement d'une information, transmet son analyse aux services concernés. Parallèlement, le service Tracfin reçoit les demandes entrantes sur des objectifs définis par les services de renseignement afin d'apporter son expertise sur les points demandés.

La loi relative au renseignement du 24 juillet 2015 définit les techniques de surveillance dont Tracfin peut disposer, ainsi que le régime d'autorisation (finalité, durée, conservation et destruction des données). Parmi les techniques de recueil de renseignement permises par cette loi, Tracfin recourt en priorité aux dispositifs permettant l'accès aux réseaux des opérateurs de télécommunications pour le suivi d'individus identifiés comme présentant une menace terroriste.

Afin d'améliorer son efficacité et de favoriser une utilisation optimale des données reçues, Tracfin a entrepris, fin 2014, un projet stratégique de refonte de son système d'information opérationnel autour de trois chantiers :

• *la collecte* : évolution du portail ERMES afin qu'il puisse accueillir un flux d'informations plus important tout en maintenant un haut niveau de sécurité, et permette l'interconnexion avec des partenaires publics (nationaux ou internationaux) et privés ;

• *l'analyse* : mise en place d'une infrastructure innovante pour l'analyse de données afin d'enrichir les déclarations de soupçon à partir du patrimoine d'informations détenu par le service ;

• *la visualisation* : développement de nouveaux outils de recherche pour les analystes et enquêteurs de Tracfin permettant d'adapter les « process métiers » aux enjeux du service. Ce nouveau système d'information sera mis en place à la fin de l'année 2017.

En termes de coopération internationale, Tracfin est fortement impliqué :

– *au sein du GAFI*, instance dans laquelle le service, qui fait partie de la délégation française, est en charge des travaux menés par le groupe de travail sur les typologies. En 2015, un agent de Tracfin a été mandaté, avec un représentant des États-Unis, pour rédiger un rapport sur les risques émergents en matière de financement du terrorisme. Ce rapport a été publié en octobre 2015. Tracfin a également participé à l'élaboration d'une étude sur le financement de Daech ;

– *au sein du groupe Egmont*, en charge de l'échange opérationnel d'informations entre les 154 cellules de renseignement financier existantes dans le monde. Tracfin s'attache à faire en sorte que les échanges opérationnels aient lieu dans des délais très rapides.

Par son action, Tracfin œuvre à la levée des entraves à la coopération internationale en promouvant, par exemple, le droit de communication de chaque cellule, l'accès direct aux données, et l'existence d'un fichier central des comptes des personnes morales et physiques.

B. AUTRES SERVICES CONCOURANT AU RENSEIGNEMENT

1. Le renseignement territorial

Le recueil du renseignement de premier niveau est réalisé par deux services [(1)] : le Service central du renseignement territorial (héritier des renseignements généraux et qui relève de la Direction générale de la Police nationale) et la Sous-direction de l'anticipation opérationnelle (qui relève de la Direction générale de la Gendarmerie nationale). Ils appartiennent au « second cercle » de la communauté du renseignement et sont donc régis par l'article L. 811-4 du code de la sécurité intérieure (en ce qui concerne l'utilisation des techniques de renseignement).

a. Le Service central du renseignement territorial

Aux termes du décret du 27 juin 2008 complété par le décret du 9 mai 2014, la Direction centrale de la sécurité publique est placée, au sein de la Direction générale de la Police nationale, sous l'autorité d'un directeur de service, secondé à la fois par un directeur central adjoint et par un directeur central adjoint chargé du renseignement. Ce dernier est le chef du Service central du renseignement territorial, succédant à la sous-direction de l'information générale (SDIG).

Le SCRT assure le recueil des renseignements les plus importants provenant des services départementaux du renseignement territorial (SDRT) ou des antennes de renseignement territorial (ART).

Tous les renseignements recueillis localement par les services du renseignement territorial font l'objet d'une exploitation en lien avec les services de police et de gendarmerie, d'une transmission au SCRT et d'une information des bureaux zonaux de liaison et de coordination (BZLC) qui sont des structures départementales et régionales dans lesquelles les représentants du renseignement territorial et ceux de la DGSI se livrent à des échanges quotidiens.

Le SCRT réalise, sous le double timbre de la Police et de la Gendarmerie nationales, des notes de synthèse destinées aux décideurs politiques et opérationnels, ainsi qu'aux principaux services de renseignement concernés par les thématiques abordées. La DGSI est systématiquement destinataire de ces documents.

Ce service est également doté d'une division nationale de recherche et d'appui qui gère les surveillances humaines et techniques. Le législateur a pleinement validé cette capacité en autorisant le renseignement territorial à avoir accès à toutes les techniques de renseignement dans les trois thématiques de son

(1) On laissera de côté la Direction du renseignement de la Préfecture de Police qui exerce, à Paris et au sein de la petite couronne, les missions du service du renseignement territorial.

cœur de métier que sont les dérives urbaines, la contestation violente et la prévention de la radicalisation violente.

Par décret du 27 juillet 2015, le SCRT s'est vu reconnaître une compétence en matière de prévention du terrorisme. Dans ce cadre, le service se doit d'évaluer précisément la nature de la menace. Les personnes signalées peuvent être également inscrites au fichier des signalés pour la prévention et la radicalisation à caractère terroriste. Si le risque paraît objectif et sérieux, le dossier est transmis à la DGSI.

En termes d'effectifs, le SCRT a connu une progression significative de ses capacités depuis la création de la SDIG en 2008, date à laquelle le service était passé de 3 900 à 1 400 agents. En neuf ans, le renseignement territorial a été renforcé de plus de 1 100 ETPT. Au 1er janvier 2017, sur les 2 592 agents qui composent le service, 251 sont affectés en centrale et 2 341 dans les territoires, au sein des services de sécurité publique (179 implantations), de Gendarmerie (49 implantations, 14 supplémentaires en 2017) et, depuis le 1er septembre 2016, dans les aéroports nationaux (4 implantations, 5 supplémentaires en 2017).

S'agissant des capacités, le maillage territorial du SCRT est la première priorité – raison pour laquelle la dernière tranche de renfort du plan de lutte contre le terrorisme, prévue au printemps 2017, permettra à tous les Services départementaux du renseignement territorial de métropole et d'Outre-mer d'atteindre le seuil de 10 effectifs actifs par service, et de couvrir ainsi l'ensemble du domaine de compétence.

Une seconde priorité tient à la difficulté que rencontre le SCRT à avoir accès au renseignement issu des procédures judiciaires antiterroristes. Ainsi, pour n'évoquer que les enquêtes les plus récentes, le SCRT n'a eu accès à aucune information sur les enquêtes conduites à la suite des trois attentats de Magnanville, de Nice et de Saint-Etienne du Rouvray, et il n'a donc pas été en mesure de fournir à ses effectifs sur le terrain des renseignements ou des grilles d'analyse ou d'alerte leur permettant de progresser dans la prévention de ce type d'actes – alors même que le *modus operandi* de Nice s'est déjà reproduit à Berlin.

Cette préoccupation a été prise en compte par la loi du 28 février 2017 relative à la sécurité publique. Cette loi autorise désormais l'accès des services de renseignement du « premier cercle » aux informations recueillies dans le cadre des procédures judiciaires antiterroristes. Elle vise également, selon certaines modalités, le « second cercle » et notamment le renseignement territorial dont les 2 592 agents sont autant de capteurs de premier niveau dans le domaine de la prévention du terrorisme.

b. La sous-direction de l'anticipation opérationnelle

La Sous-direction de l'anticipation opérationnelle est régie par les dispositions de l'article 17-1 de l'arrêté du 12 août 2013 (modifié par l'arrêté du 6 décembre 2013).

La SDAO est chargée du pilotage du renseignement opérationnel au sein de la Gendarmerie nationale en s'appuyant sur la base de données de sécurité publique (BDSP), alimentée par tous les militaires de l'institution au cours de l'exécution de leur mission, et sur la chaîne du renseignement opérationnel formée par les cellules et par les bureaux de renseignement (respectivement situés dans les départements et dans les régions).

La SDAO contribue à l'exécution de la mission de renseignement territorial. Elle assure le lien fonctionnel, au niveau central, avec le SCRT. Elle garantit également l'efficience du partage du renseignement entre les échelons territoriaux de commandement de la Gendarmerie nationale (cellules et bureaux de renseignement) et les échelons déconcentrés du renseignement territorial (services départementaux, régionaux et zonaux).

Elle pilote le recueil, l'exploitation et l'analyse du renseignement de défense, de sécurité nationale et d'ordre public nécessaires à l'exécution des missions de la Gendarmerie.

L'exercice de la mission de renseignement opérationnel au sein de la Gendarmerie repose sur :

– le maillage territorial des brigades de Gendarmerie ;

– les Gendarmeries spécialisées ;

– et le déploiement de gendarmes à l'étranger, ainsi que sur les théâtres extérieurs.

La SDAO dispose d'une chaîne d'analyse et d'anticipation (540 analystes) articulée comme suit :

– les cellules de renseignement dans les départements ;

– les bureaux de renseignement dans les régions ;

– et la SDAO elle-même, au sein de la Direction générale.

Le recueil des informations est :

– réalisé par chaque militaire dans le cadre de ses missions quotidiennes ;

– et animé par les différents échelons de commandement ;

– en particulier, un officier adjoint de renseignement (OAR) assiste le chef territorial (zonal, régional, ou départemental) dans le domaine de l'animation (interne) du renseignement et dans celui de l'échange avec les services partenaires ;

– les groupes d'évaluation départementaux sont, par exemple, le cadre d'intervention de ces OAR, dans le secteur spécifique de la prévention de la radicalisation et de l'alimentation du FSPRT.

Enfin, l'information est intégrée dans la base de données de sécurité publique (BDSP) en vue de son exploitation et de son analyse.

2. Le développement des capacités du renseignement pénitentiaire

Au regard de l'importance des phénomènes de radicalisation susceptibles d'intervenir au sein des établissements pénitentiaires, il importe d'accorder une attention particulière à la question du renseignement pénitentiaire, dans le droit fil de l'intégration du service chargé de cette mission, par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, au « deuxième cercle » de la communauté du renseignement. Cette problématique a du reste été mise en exergue par le ministère de la justice avec la présentation par le Garde des Sceaux, le 25 octobre 2016, d'un plan pour la sécurité pénitentiaire et l'action contre la radicalisation violente, qui a notamment modifié la doctrine relative à la gestion des détenus radicalisés ou en voie de radicalisation.

Le cœur du renseignement pénitentiaire est constitué, au sein de la direction de l'administration pénitentiaire du ministère de la justice, par le bureau du renseignement pénitentiaire. Ce dernier, créé en 2003, a pour mission de suivre et d'analyser les informations recueillies en prison, et également de favoriser la prise de décision des hautes autorités à partir de l'étude de ces données. Compte tenu de l'importance de la menace terroriste, il a été décidé de mieux intégrer désormais ce bureau au sein du système pénitentiaire et d'amplifier considérablement ses moyens d'action.

La réforme va entrer progressivement en vigueur au cours de l'année 2017. Elle s'accompagne de la mobilisation de crédits budgétaires, pour un montant de 12 millions d'euros, qui seront engagés au titre de cet exercice.

Les principales caractéristiques de la réforme sont les suivantes :

– par le décret n° 2016-1877 du 27 décembre 2016 relatif au ressort territorial, à l'organisation et aux attributions des directions interrégionales des services pénitentiaires (DISP) et de la mission des services pénitentiaires de l'outre-mer, le Gouvernement a ajouté les trois nouvelles finalités au service du renseignement pénitentiaire que sont la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisée ainsi que la prévention des évasions

maintien du bon ordre et de la sécurité dans les établissements destinés à recevoir des personnes détenues. Ce texte réglementaire donne par ailleurs une existence administrative et définit le périmètre de compétence des cellules interrégionales du renseignement pénitentiaire (CIRP) qui sont intégrées au sein des DISP ;

– par le décret n° 2017-37 du 16 janvier 2017, ces mêmes finalités ont été inscrites dans les missions confiées à la direction de l'administration pénitentiaire (modification du décret du 9 juillet 2008 relatif à l'organisation du ministère de la Justice) ;

– l'arrêté du 16 janvier 2017 modifiant l'arrêté du 30 juin 2015 fixant l'organisation en sous-directions de la direction de l'administration pénitentiaire a quant à lui créé une sous-direction de la sécurité pénitentiaire notamment chargée de piloter et d'évaluer « *l'action de l'administration pénitentiaire en matière de lutte contre le terrorisme et contre la radicalisation violente* » et de superviser « *les activités de renseignement pénitentiaire* », d'animer « *le réseau des cellules interrégionales de renseignement pénitentiaire et des délégués locaux du renseignement pénitentiaire* », de « *centraliser les demandes de mise en œuvre des techniques de recueil du renseignement légalement autorisées à l'égard des personnes confiées à l'administration pénitentiaire par l'autorité judiciaire* », de contrôler « *les actions déployées en ce domaine* », d'évaluer « *leur mise en œuvre* », de synthétiser et de diffuser « *les informations et renseignements collectés* » ;

– dans le droit fil de cette réforme, le bureau du renseignement pénitentiaire est devenu un bureau central du renseignement pénitentiaire (BCRP) qui regroupe 17 personnels. Ces effectifs seront portés à 40 d'ici à la fin de l'année 2017 ;

– le BCRP a notamment pour missions de piloter la politique de renseignement pénitentiaire définie par le Garde des Sceaux, et notamment d'animer le réseau composé des CIRP et des locaux du renseignement affectés dans les établissements. Il participe aux travaux du comité de pilotage de la lutte contre le terrorisme et la radicalisation violente qui rassemble l'ensemble des directions du ministère et à ceux du conseil scientifique composé de représentants de toutes les disciplines pouvant œuvrer dans ce domaine (sociologie, psychologie, sciences cognitives et comportementales, etc.). Il est également destiné à assurer l'interface avec les services membres de la communauté du renseignement et les services du deuxième cercle ;

– dans ce cadre, le BCRP dispose, depuis le 3 janvier 2017, d'un officier de liaison provenant de la DGSI ; il sera prochainement suivi par des officiers de liaison provenant du service central du renseignement territorial et de la SDAO. Par ailleurs, un fonctionnaire du BCRP rejoindra la cellule INTERSERVICES au cours du second semestre 2017 tandis qu'un autre sera mis à la disposition de la DRPP ;

– par le décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure, les fonctionnaires du BCRP et des CIRP se sont vus reconnaître l'accès à certaines techniques de recueil de renseignement pour les finalités « prévention du terrorisme » et « prévention de la criminalité et de la délinquance organisées » ;

– s'agissant de la mise en œuvre des techniques de recueil de renseignement pour l'exercice des missions spécifiques de l'administration pénitentiaire tendant à prévenir les évasions et à assurer le bon ordre au sein des établissements pénitentiaires, une clarification des dispositions législatives du code de procédure pénale et du code de la sécurité intérieure s'imposait. À cet effet, sur proposition du Gouvernement, un article 9 *bis* a été inséré dans le projet de loi relatif à la sécurité publique, définitivement adopté par le Parlement le 16 février dernier, afin de clarifier les règles et modalités de mise en œuvre des techniques de recueil de renseignement au sein des établissements pénitentiaires qui résultaient de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale ;

– a ainsi été introduit dans le livre VIII du code de la sécurité intérieure, un titre V *bis* intitulé « du renseignement de sécurité pénitentiaire » permettant la mise en œuvre de certaines techniques de recueil de renseignement (accès aux données de connexion, géolocalisation en temps réel sur sollicitation du réseau, pose de balises, captation des données de connexion par *IMSI catcher* et interceptions de sécurité) par certains fonctionnaires du BCRP et des CIRP pour les finalités liées à la prévention des évasions et au maintien du bon ordre au sein des établissements pénitentiaires ;

– au sein des DISP, les CIRP s'appuient déjà sur un réseau de 42 fonctionnaires ;

– s'agissant des établissements pénitentiaires, on dénombre 177 délégués locaux du renseignement répartis au sein de 188 établissements. Ces délégués locaux sont des personnels de surveillance (souvent des officiers) spécialement formés aux missions de renseignement. Le maillage de ce réseau reste néanmoins encore insuffisant : à titre d'exemple, la maison d'arrêt de Fleury-Mérogis ne compte que *** délégués pour 4 000 détenus, celle de Fresnes, *** pour près de 2 500 détenus. Il convient donc de renforcer sans délai ce réseau ;

– les personnels chargés d'une mission de renseignement se verront dispenser des formations spécifiques tout au long de l'année 2017.

La population suivie par le renseignement pénitentiaire présente les caractéristiques suivantes :

– sur les 68 560 personnes écrouées détenues, 2 811 personnes sont des détenus particulièrement signalés (DPS) ;

– parmi ces 2 811 DPS, on dénombre :

– 390 personnes détenues pour des faits de terrorisme en lien avec l'islam radical (dont 308 prévenus) ;

– 1 329 personnes détenues, prévenues ou condamnées pour des faits de droit commun, signalées comme susceptibles de s'inscrire dans une démarche de radicalisation.

– en outre, 412 personnes radicalisées sont suivies en milieu ouvert par les services pénitentiaires d'insertion et de probation (SPIP), dont 108 sous contrôle judiciaire pour des affaires liées au terrorisme.

– le suivi de ces personnes par les services du renseignement pénitentiaire fera l'objet d'un traitement automatisé de données à caractère personnel dénommé « collecte analyse renseignement » (CAR).

Proposition 8. Après la finalisation du cadre juridique, les moyens humains et matériels dédiés au renseignement pénitentiaire doivent poursuivre leur montée en puissance au cours des années à venir. La Délégation parlementaire au renseignement accordera une attention particulière à la mise en œuvre de la réforme au cours de l'année à venir.

C. TROIS PROBLÈMES TRANSVERSAUX PROPRES AUX SERVICES DE RENSEIGNEMENT

Au cours des entretiens que la DPR a conduit, tout au long de l'année, avec les services de renseignement, plusieurs problèmes récurrents se sont fait jour, indépendamment des difficultés ponctuelles propres à tel ou tel service. On distinguera la question des personnels, celle des fichiers, et celle des renseignements qui peuvent être obtenus par les juges au cours de leurs instructions.

1. Les personnels

Les recrutements dans les services de renseignement sont actuellement importants ; néanmoins les services rencontrent certaines difficultés :

– difficultés liées au caractère limité du vivier des candidats dans certaines spécialités recherchées, notamment les ingénieurs informatiques, d'autant que de nombreuses autres administrations de l'État prospectent des profils analogues, sans compter les entreprises en mesure d'offrir des niveaux de rémunération nettement plus élevés ;

– difficultés pour recruter des personnels parlant certaines langues rares ;

– rigidités des règles de la fonction publique pour embaucher et fidéliser des contractuels ;

– manque de moyens en analystes pour l'exploitation.

Pour résoudre correctement ces difficultés, il serait utile de procéder à une analyse générale et exhaustive portant sur les questions de recrutement, de rémunération et de carrière au sein des services de renseignement. Cette étude pourrait être confiée à l'Inspection des services de renseignement sous couvert du Premier ministre.

En particulier, l'ISR pourrait se prononcer sur la question qui consiste à savoir si, dans certains cas, il ne serait pas possible de généraliser à l'ensemble de la communauté du renseignement certains types de contrats qui sont utilisés dans certains services (par exemple à la DGSE) ; ou encore, s'il ne conviendrait pas – en réponse à des situations exceptionnelles – de définir certaines règles particulières, éventuellement dérogatoires par rapport aux règles de la fonction publique.

Proposition 9. Il convient de confier à l'ISR une étude portant sur les questions liées aux recrutements, aux rémunérations et aux carrières des personnels des services de renseignement.

2. Les fichiers

Actuellement, la question des fichiers se pose principalement pour la lutte antiterroriste.

À l'origine, le fichier des personnes recherchées (FPR), qui relève de la Direction générale de la police nationale, est le fichier dans lequel sont inscrits les individus faisant l'objet de signalement à divers titres, administratifs ou judiciaires.

Créé en 1969, il comporte plus de 400 000 noms, qu'il s'agisse de mineurs en fugue, d'évadés de prison, de membres du grand banditisme, de personnes empêchées de quitter le territoire national du fait d'une décision de justice, ou d'activistes.

Les personnes suspectées de terrorisme sont recensées dans ce fichier au moyen d'une fiche S – la lettre S signifiant « atteinte à la sûreté de l'État ». Au sein du FPR, les fiches S sont au nombre de 12 000.

Les inscriptions de la catégorie S (ou fiches S) concernent :

– les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État et à la sécurité publique, par le recours ou le soutien actif apporté à la violence ;

– ainsi que celles qui entretiennent des relations directes et non fortuites avec ces personnes.

Une fiche S peut donc aussi bien concerner un objectif identifié d'un service qu'une personne de son entourage dont le contrôle serait de nature à apporter des informations utiles concernant l'objectif « primaire ».

Par ailleurs, les fiches S ne se réduisent pas à la seule problématique du contre-terrorisme. Ainsi, au regard de ses missions et des possibilités offertes par le FPR, la DGSI utilise également la mise en surveillance de personnes au sein de ce fichier dans le cadre de ses autres missions : le contre-espionnage, la lutte contre les extrémismes violents, la lutte contre les organisations terroristes autres que sunnites et, de manière plus réduite, la contre-prolifération et la lutte contre la criminalité organisée.

Toutefois, en raison de la montée de l'islamisme radical, les pouvoirs publics ont estimé que le FPR n'était plus un instrument suffisamment efficace.

Le cas d'un terroriste – Yassin Salhi – l'illustre. Celui-ci est passé à l'acte en 2015 en Isère. Il avait été fiché S de 2006 à 2008. Néanmoins, compte tenu de l'absence d'éléments d'information corroborant une dérive radicale après 2008, la fiche S le concernant avait été supprimée. Elle n'existait donc plus dans le fichier au moment de l'attentat. Par suite, faute de fiche, l'éventualité d'une surveillance exercée sur cette personne, à défaut d'un nouveau signalement, était quasiment nulle.

En 2015, le ministère de l'Intérieur a donc souhaité créer un fichier visant à recenser l'ensemble des objectifs signalés radicalisés et permettant de s'assurer que leur prise en compte est effective par un service – ce fichier s'apparentant à un outil centralisé de gestion du suivi des objectifs.

Cette tâche a été effectuée par l'EMOPT qui regroupe la DGSI, le service du renseignement territorial, la police judiciaire, la Préfecture de police et la Gendarmerie. Le fichier ainsi obtenu est le fichier des signalés pour la prévention de la radicalisation à caractère terroriste. Il comporte environ 15 000 noms.

Ce fichier reste par définition lié au renseignement intérieur, ce qui pose la question de sa coordination avec ceux tenus par d'autres services de renseignement ne participant pas aux travaux de l'EMOPT.

Il en va de même, d'ailleurs, concernant la coordination de l'ensemble des fichiers de renseignement entre eux, ainsi que pour la coordination de ces fichiers

avec le système d'exploitation des données des passagers aériens – le PNR – lorsque ce dernier sera définitivement mis en place.

Cette question de l'articulation des différents fichiers pose de délicates questions pratiques et juridiques. Aussi la Délégation parlementaire au renseignement souhaiterait-elle qu'une étude soit confiée à l'Inspection des services de renseignement.

Proposition 10. Il serait souhaitable que l'ISR réalise une étude sur les différents fichiers des services de renseignement, portant notamment sur leur organisation et sur leur coordination.

3. La communication aux services de renseignement d'éléments tirés des procédures pénales dans le domaine du terrorisme

La politique de lutte antiterroriste constitue l'un des domaines dans lequel il apparaît nécessaire de favoriser une fluidité et une complémentarité entre, d'une part, les actions de police administrative menées par les services de renseignement et, d'autre part, la répression des infractions terroristes, ce deuxième volet présentant du reste lui aussi une dimension préventive au regard des caractéristiques de l'infraction d'association de malfaiteurs en relation avec une entreprise terroriste [(1)].

En droit, les services de renseignement peuvent judiciariser les informations recueillies à l'occasion de l'exercice de leurs missions (notamment avec la mise en œuvre des techniques de recueil de renseignement dans les conditions prévues par le livre VIII du code de la sécurité intérieure) en application de l'article 40, alinéa 2, du code de procédure pénale [(2)], dans la mesure où ces informations révèlent l'existence d'une infraction terroriste ou sa préparation. La mise en œuvre de cette procédure implique que les informations transmises à l'autorité judiciaire fassent l'objet d'une déclassification pour celles d'entre elles qui seraient couvertes par le secret de la défense nationale et qu'elles ne révèlent pas les modes d'acquisition du renseignement (identité des sources, techniques utilisées, etc.). De même, les services de renseignement sont amenés à répondre régulièrement aux sollicitations de l'autorité judiciaire quand ils sont saisis de réquisitions.

À l'inverse, les enquêtes préliminaires conduites par le parquet de Paris ou les informations judiciaires conduites par le pôle d'instruction antiterroriste du tribunal de grande instance de Paris peuvent conduire les enquêteurs et magistrats à recueillir des éléments pouvant être utiles à l'exercice des missions exercées par les services de renseignement dans le domaine de la prévention du terrorisme. Or,

(1) Infraction-obstacle qui permet de judiciariser un dossier au stade de la préparation de l'acte de terrorisme.

(2) En vertu duquel, « 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 ».

en l'état de la législation actuelle, aucune disposition n'autorise de telles transmissions dans la mesure où les éléments tirés d'une procédure sont couverts par le secret de l'enquête ou de l'instruction, comme la DPR l'avait souligné devant le Garde des Sceaux lors de son audition.

Depuis, considérant qu'un tel vide juridique était de nature à réduire l'efficacité de la politique de lutte antiterroriste, les commissions des lois des deux assemblées parlementaires se sont mises d'accord pour introduire un dispositif spécifique dans la loi relative à la sécurité publique, définitivement adoptée par le Parlement le 16 février dernier. L'article 6 *bis* de ce texte, qui introduit un article 706-25-2 dans le code de procédure pénale, ouvre ainsi, sous certaines conditions, l'accès des services de renseignement aux informations contenues dans les procédures antiterroristes.

Si le principe du secret de l'enquête et de l'instruction constitue une règle essentielle permettant de garantir la sérénité des investigations judiciaires, il est néanmoins apparu qu'une telle règle ne présentait pas un caractère absolu et comportait d'ores et déjà certaines dérogations, notamment lorsqu'il s'agit d'une communication restreinte à une personne habilitée à en connaître. À titre d'exemple, le législateur a prévu des dérogations spécifiques, notamment à l'article 11-2 du code de procédure pénale créé par la loi du 14 avril 2016, qui permet à l'administration d'être informée de certains éléments d'une procédure en cours concernant une personne qu'elle emploie.

Ce raisonnement a ainsi conduit le législateur à prévoir la possibilité d'une communication aux services spécialisés de renseignement des éléments de toute nature (procès-verbaux d'audition, copie du contenu de certains supports, y compris numériques) figurant dans les procédures judiciaires portant sur des actes de terrorisme, tout en laissant à l'autorité judiciaire (procureur de la République de Paris ou juge d'instruction en charge du dossier) le soin d'apprécier si une telle communication n'est pas de nature à nuire à l'efficacité de la procédure pénale. Ce dispositif précise par ailleurs que les informations communiquées peuvent être transmises aux services appartenant au « deuxième cercle » lorsqu'elles sont nécessaires à l'exercice des missions de ces derniers en matière de prévention du terrorisme mais qu'elles ne peuvent faire l'objet d'un échange avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement. Il dispose enfin que les agents des services destinataires des communications des autorités judiciaires sont tenus par le secret professionnel à l'égard des informations reçues, dans les conditions et sous les peines prévues aux articles 226-13 et 226-14 du code pénal.

D. UNE ORGANISATION DES SERVICES À CONSOLIDER

La place importante du renseignement dans la prévention et la lutte contre le terrorisme a été mise en lumière par la communication gouvernementale, mais aussi à l'occasion des travaux des assemblées parlementaires, notamment des missions d'information et commissions d'enquête conduites à l'Assemblée

nationale et au Sénat, ainsi que dans de nombreux articles de presse et publications d'experts.

Soulignant naturellement certaines faiblesses des services de renseignement, notamment dans leur coordination, nombre de publications ont appelé à des réorganisations plus ou moins profondes des services, considérées souvent comme le remède miracle apportant une solution à des phénomènes qui dépassent largement la seule action des services de renseignement et auxquels les services, d'ailleurs, s'adaptent souvent avec une très grande réactivité.

Trois axes de réformes sont fréquemment avancés.

Le premier auquel la Délégation a apporté une réponse réservée et prudente dans son rapport pour 2015 [(1)], consiste en la mise en place d'une agence technique indépendante, gestionnaire de l'ensemble des moyens techniques et pourvoyeuse des différents services spécialisés à l'instar des modèles américains (NSA) et britannique (GCHQ). En France, l'État s'est engagé dans un processus de mutualisation des moyens techniques pour éviter des duplications coûteuses entre les services et pour en assurer la supervision. Les moyens restent au sein des services qui en sont les principaux utilisateurs, mais ceux-ci peuvent être mis à disposition de ceux qui en ont besoin ; leur modernisation est conduite par un comité de pilotage supervisé par le Coordonnateur national du renseignement et financée par des crédits interministériels. Les deux solutions ont leurs avantages et inconvénients.

Le second consiste en la fusion des services du renseignement territorial, le Service central du renseignement territorial et la Sous-direction de l'anticipation opérationnelle de la Gendarmerie nationale, au sein d'une nouvelle direction générale du renseignement territorial placée directement auprès du ministre de l'Intérieur ; cette nouvelle direction reprendrait les attributions de la Direction du renseignement de la préfecture de police de Paris en matière d'information générale et sa mission de lutte antiterroriste serait confiée à une direction zonale de la DGSI. La nouvelle direction générale du renseignement territorial serait intégrée comme un septième service spécialisé au sein de la communauté du renseignement.

« *Passer de quatre à deux services de renseignement intérieur ne signifie pas ressusciter la dualité « DST-RG » en créant un service concurrent de la DGSI : celle-ci demeurerait le chef de file du renseignement intérieur, avec un droit d'évocation sur les dossiers du renseignement territorial. L'enjeu est plutôt de prendre en compte dans notre organisation administrative, la pérennité d'une menace diffuse sur le territoire national et la nécessité de disposer d'un renseignement de proximité pleinement outillé pour y répondre* » [(2)].

---

(1) Rapport d'activité 201, p. 54 et suivantes.

(2) Assemblée nationale n° 3922 - Rapport de la commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015 (Georges Fenech, président, Sébastien Pietrasanta, rapporteur) -5 juillet 2016, p. 186 et suivantes.

La Délégation reste toutefois dubitative sur l'opportunité d'une nouvelle réforme du renseignement intérieur et du renseignement territorial après celle de 2013-2014 ; trop de réformes successives nuit à l'efficacité des services et à leur coordination, même s'il s'agit de mettre en place une ligne hiérarchique plus forte. En outre, les services en charge du renseignement territorial sont organisés de façons différentes selon leurs entités de rattachement (Police ou Gendarmerie) et travaillent en liens directs et étroits avec les unités de terrain, qu'elles appartiennent à d'autres directions au sein de la DGPN ou de la DRPP ou à la même direction (cas des brigades de Gendarmerie). Sauf à doter le nouveau service spécialisé de ressources humaines très importantes, bien au-delà des créations d'emplois déjà conséquentes opérées depuis 2014, l'ensemble risque de perdre en efficacité dans la collecte de l'information de proximité qui repose sur un maillage beaucoup plus vaste que les seuls services en charge du renseignement territorial, c'est-à-dire sur l'ensemble des unités de base de la Police et de la Gendarmerie.

Le troisième axe consiste à créer une agence nationale de lutte contre le terrorisme placée auprès du Premier ministre [(1)]. Depuis le Conseil national du renseignement du 13 janvier 2016, sur le territoire national « *le pilotage opérationnel quotidien de la stratégie de lutte contre le terrorisme est placé sous l'autorité directe du ministre de l'Intérieur avec le concours de l'ensemble de la communauté française du renseignement* ». Il a ainsi été acté le *leadership* de la DGSI dans la définition de la manœuvre globale de la lutte antiterroriste. Pour autant, pour les partisans d'une agence nationale, la définition de la stratégie doit englober l'ensemble des services concourant à la lutte contre le terrorisme, et relève davantage d'une entité interministérielle que de l'action d'un « chef de file ministériel », quand bien même il serait reconnu au plus haut niveau de l'État.

Les partisans de cette proposition la prolongent par une autre réforme ambitieuse qui consiste à transformer le Coordonnateur national du renseignement en un véritable directeur national du renseignement directement rattaché au Premier ministre qui disposerait de l'agence, mais aussi de l'Inspection et de l'Académie du renseignement [(2)]. Ce directeur national aurait vocation à arbitrer les budgets des différents services et jouerait un rôle plus important dans les autorisations de mise en œuvre des techniques de renseignement. Il demeurerait le conseiller du Président de la République en matière de renseignement.

Ces réformes sont en partie inspirées par l'expérience américaine et ont le mérite d'une architecture claire, encore qu'elles modifieraient quelque peu l'équilibre institutionnel et notamment la relation toujours complexe dans la pratique constitutionnelle de la V^e^ République entre le Président de la République et le Premier ministre.

La voie choisie par les autorités de l'État est plus pragmatique et a l'avantage d'une plus grande plasticité pour s'adapter aux évolutions de la menace. Elle a

(1) Assemblée nationale n° 3922 précité, p.189 et suivantes.
(2) Assemblée nationale n° 3922 précité, p.192 et suivantes.

consisté depuis 2014 à augmenter les moyens de l'ensemble des services (moyens humains, moyens financiers, moyens techniques et moyens législatifs), et plus particulièrement de ceux en charge du renseignement territorial, à mettre en place des outils de coordination opérationnelle entre les services (cellules spécialisées avec un service chef de file) et à instaurer un *management* renforcé fondé sur un pilotage politique partant du Conseil de défense et de sécurité nationale, auquel participent désormais systématiquement le ministre de l'Intérieur et celui de la Justice, ainsi que les directeurs des principaux services spécialisés, passant par le ministre de l'Intérieur, dont le *leadership* est affirmé et qui dispose d'un état-major spécialisé (EMOPT), jusqu'aux préfets de zone et de département qui animent localement, de façon hebdomadaire, des cellules opérationnelles auxquelles participent les représentants des services de renseignement et d'autres administrations déconcentrées de l'État, avec pour mission de détecter les signaux faibles de radicalisation et de répartir entre les services l'évaluation et le suivi des personnes radicalisées. Parallèlement et en complémentarité avec le Conseil national de défense et de sécurité nationale, qui porte sur l'état de la menace et l'engagement de nos forces armées sur les théâtres extérieurs, le Conseil national du renseignement se réunit régulièrement, deux à trois fois par an, afin de permettre au Président de la République, sur proposition du Coordonnateur national du renseignement, d'opérer les grandes orientations de la politique de renseignement et de fixer les priorités d'organisation, de mutualisation et de coopération des services, afin d'assurer la cohérence du dispositif. Le Coordonnateur est chargé de suivre l'application des décisions prises. Cette nouvelle chaîne de travail mérite d'être confortée, éprouvée et évaluée.

S'il est parfaitement légitime, à l'heure où l'imbrication des menaces est forte et au moment des échéances électorales, que certains s'interrogent sur la pertinence de l'organisation de la politique publique du renseignement, la Délégation estime toutefois qu'il n'est pas raisonnable d'entrer dans la voie d'une réorganisation aussi ambitieuse et structurante alors que les services sont mobilisés de façon intense et quotidienne dans la lutte contre le terrorisme. Une telle réorganisation risque, en effet, de mobiliser beaucoup d'énergie au prix d'un affaiblissement, si temporaire soit-il, des capacités opérationnelles. L'enjeu est davantage dans l'échange, le partage de l'information et des analyses, la fluidité des communications, que dans l'architecture générale. Néanmoins, à la lumière de l'expérience, passé cette période intense, il conviendra d'en tirer les leçons et de ne pas exclure *a priori* de la réflexion une évolution, à froid, de l'architecture d'ensemble. Cette réflexion devra, en outre, être conduite en prenant en considération l'ensemble des menaces auxquelles est confronté notre pays. Si la lutte contre le terrorisme, qui est aujourd'hui prioritaire, rend nécessaire des adaptations, celles-ci ne sauraient être constitutives d'un affaiblissement de nos services dans leurs autres domaines de compétence. C'est pourquoi, à ce stade, la Délégation ne propose pas de réorganisation d'ensemble des services.

IV. UN PREMIER BILAN DES DEUX LOIS DU 24 JUILLET ET DU 30 NOVEMBRE 2015 AU TERME D'UNE ANNÉE D'APPLICATION

L'utilisation de certaines techniques de renseignement a été encadrée par deux lois – la loi n° 2015-912 du 24 juillet 2015 relative au renseignement et la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

Dans les pages qui suivent nous allons examiner ces deux lois tour à tour ; puis, nous aborderons la question de l'exception hertzienne, exception dont le fondement juridique était l'article L. 811-5 du code de la sécurité intérieure, mais qui a été invalidée par la décision n° 2016-590 QPC du 21 octobre 2016 du Conseil constitutionnel. Enfin, nous tirerons le bilan de ces deux lois après une année d'application.

A. LA LOI DU 24 JUILLET 2015

La loi précise les conditions d'utilisation sur le territoire national de certaines techniques de renseignement. Ces techniques ne s'appliquent qu'en l'absence de procédure judiciaire portant sur les mêmes faits et le texte fixe la procédure d'autorisation pour leur mise en œuvre. Il détaille en outre précisément les techniques de renseignement soumises à une autorisation préalable. Enfin, la loi est assortie de garanties importantes pour les citoyens.

1. Une clarification bienvenue des conditions d'utilisation des techniques de renseignement

La loi du 24 juillet 2015 fixe très précisément les missions assignées aux services de renseignement et, par conséquent, les hypothèses dans lesquelles l'utilisation des techniques de renseignement est licite.

Les missions des services de renseignement sont décrites dans l'article 2 de la loi (article L. 811-3 du code de la sécurité intérieure). Ces missions visent à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :

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

– les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

– les intérêts économiques, industriels et scientifiques majeurs de la France ;

– la prévention du terrorisme ;

– la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, ainsi que des violences collectives de nature à porter gravement atteinte à la paix publique ;

– la prévention de la criminalité et de la délinquance organisées ;

– la prévention de la prolifération des armes de destruction massive.

En conséquence, l'article L. 811-3 du code de la sécurité intérieure indique que ces motifs sont les seuls qui peuvent être retenus par les services de renseignement pour recourir à l'emploi des techniques de renseignement soumises à autorisation.

Par ailleurs, l'article 1er de la loi du 24 juillet 2015 (article L. 801-1 du code de la sécurité intérieure) détaille les modalités selon lesquelles ces techniques de renseignement peuvent être décidées et mises en œuvre :

– la décision et la réalisation des investigations doivent procéder d'une autorité ayant légalement compétence pour le faire ;

– elles doivent résulter d'une procédure conforme aux prescriptions de l'article 2 de la loi relative au renseignement ;

– elles doivent respecter les missions propres de chaque service de renseignement ;

– elles doivent être justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure ;

– enfin, les atteintes qu'elles portent au respect de la vie privée doivent être proportionnées aux motifs invoqués.

Les conditions de mise en œuvre des techniques de renseignement sont donc très strictes. La CNCTR s'assure – au moment où elle est saisie par le Gouvernement d'une demande d'investigation dans le cadre de la procédure d'autorisation prévue par la loi – du respect de ces principes. Il en va de même pour le Conseil d'État qui statue *a posteriori* sur les éventuels recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques.

2. Une procédure d'autorisation pour la mise en œuvre des techniques de renseignement

La procédure d'autorisation pour la mise en œuvre des techniques de renseignement figure également dans l'article 2 de la loi du 24 juillet 2015. À cet égard, il convient de retenir les points suivants :

– la demande du service de renseignement doit respecter un certain nombre de prescriptions (article L. 821-2 du code de la sécurité intérieure) ; elle doit préciser la ou les techniques à mettre en œuvre ; le service pour lequel elle est présentée ; la ou les finalités poursuivies ; le ou les motifs des mesures ; la durée de validité de l'autorisation ; la ou les personnes concernées ; le ou les lieux surveillés ; éventuellement les véhicules ou autres vecteurs en cause ;

– la demande remonte au ministre qui exerce le pouvoir hiérarchique sur le service de renseignement (article L. 821-2), puis au Premier ministre (article L. 821-1) ;

– ce dernier saisit la CNCTR qui est instituée par l'article 2 de la loi relative au renseignement ;

– la CNCTR rend son avis au Premier ministre dans les 24 heures, sauf s'il s'agit d'une question complexe ; dans ce dernier cas, l'avis est rendu dans les 72 heures (article L. 821-3) ;

– avant de rendre son avis, la CNCTR vérifie que la demande respecte bien toutes les conditions de forme et de fond qui sont prévues par la loi et en particulier les dispositions de l'article L. 801-1 du code de la sécurité intérieure (article L. 833-5) ;

– au vu de l'avis de la CNCTR, le Premier ministre décide seul de la suite donnée à la demande. Il n'est pas tenu par l'avis de la Commission. En particulier, il peut délivrer l'autorisation demandée après avis défavorable de la CNCTR, mais, en ce cas, il doit indiquer les motifs pour lesquels l'avis de la Commission n'a pas été suivi (article L. 821-4) ;

– l'autorisation est ensuite transmise au ministre concerné et, par suite, au service de renseignement qui avait formulé la demande et qui sera chargé de l'exécution des mesures correspondantes (article L. 833-6).

Il convient d'observer que, lorsqu'il s'agit d'écoutes téléphoniques – l'une des techniques de renseignement soumises à autorisation les plus couramment usitées sur le territoire national –, la mission qui consiste à réaliser la captation de l'information n'est pas effectuée par le service demandeur mais par le GIC ; il s'agit d'un service du Premier ministre, créé dans les années soixante et régi aujourd'hui par les articles R. 823-1 et 2 et R. 851-6-7 et 8 du code de la sécurité intérieure – articles contenus dans le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

Le fait que les écoutes soient réalisées techniquement par un organe tiers qui n'est pas le service de renseignement demandeur, mais un service du Premier ministre, constitue un héritage de la loi n° 91-646 du 10 juillet 1991 et de ses dispositions relatives aux interceptions administratives. Pour les autres techniques de renseignement, la loi du 24 juillet 2015 a confié la réalisation de la collecte du renseignement aux services bénéficiaires, sous le contrôle de la CNCTR.

Enfin, en conclusion de ces développements consacrés à la procédure d'autorisation des techniques de renseignement, on observera que la loi a prévu également une procédure d'urgence : celle de l'article 2 (article L. 821-5 du code de la sécurité intérieure) où le Premier ministre peut délivrer, de manière exceptionnelle, en cas d'urgence absolue, et pour un nombre limité de finalités, l'autorisation demandée sans passer par la CNCTR ; toutefois, s'il utilise cette faculté, le Premier ministre doit néanmoins informer sans délai la Commission ; la CNCTR rend ensuite son avis dans les conditions de droit commun – c'est-à-dire au Premier ministre conformément à l'article L. 821-3.

3. Une énumération limitative des techniques de renseignement susceptibles d'être utilisées

L'article 5 de la loi du 24 juillet 2015 détaille un certain nombre de techniques de renseignement qui peuvent être utilisées par les services sur le territoire national, après autorisation. Ce faisant, le texte reconnaît juridiquement la possibilité pour les services de renseignement de se servir de techniques dont l'usage n'était jusqu'alors explicitement autorisé que pour l'autorité judiciaire. Les principaux articles du code de la sécurité intérieure qui concernent les techniques de renseignement sont les suivants :

– l'article L. 851-1 qui a trait au recueil des données de connexion qu'un service de renseignement peut demander aux opérateurs ;

– l'article L. 851-2 qui concerne le recueil des données de connexion en temps réel pour les seuls besoins de la lutte antiterroriste. Cet article a été modifié par l'article 15 de la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste ;

– l'article L. 851-6 qui concerne le recueil des données de connexion de manière directe par les services. Ce recueil de renseignement peut être motivé par tous les aspects de leurs missions, et non pas seulement par les finalités de la lutte antiterroriste ;

– les articles L 851-4 et L. 851-5 qui concernent les données obtenues par géolocalisation, soit par le biais de l'accès à l'équipement terminal, soit par l'usage d'une balise ;

– l'article L. 852-1 qui concerne les interceptions de correspondances et de mails, soit par le biais des interceptions de sécurité classiques, soit grâce à un outil de captation de proximité ; les conditions de mise en œuvre de cet article sont strictes ; la loi prévoit un contexte d'intervention précis ; elle réserve l'usage de ces techniques de renseignement à certaines finalités et la durée d'utilisation de ces techniques est limitée à 48 heures ;

– l'article L. 853-1 qui concerne les sonorisations de certains lieux et véhicules ;

– l'article L. 853-2 qui concerne les données stockées dans les systèmes informatiques ;

– l'article L. 853-3, enfin, qui concerne les interventions effectuées dans les lieux privés et dans les véhicules au titre de trois articles du code de la sécurité intérieure cités précédemment : les articles L. 851-5, L. 853-1 et L. 853-2.

S'agissant de ce dernier dispositif, il convient de noter que, lorsqu'il est prévu la mise en œuvre de l'un de ces trois articles (ou des trois articles à la fois) dans un lieu privé à usage d'habitation et que l'avis de la CNCTR est défavorable, le Premier ministre ne peut passer outre qu'en cas d'avis favorable du Conseil d'État – sauf s'il s'agit d'une affaire qui concerne le terrorisme et que le Premier ministre a ordonné la réalisation immédiate de l'intervention.

4. Un renforcement significatif des garanties pour les citoyens

La loi du 24 juillet 2015 prévoit des garanties et plusieurs voies de recours.

Tout d'abord, la loi a prévu une limitation de la durée de conservation des données. En effet, outre l'intervention pour avis de la CNCTR préalable à la décision du Premier ministre, outre ses capacités d'information et de contrôle, voire de saisine du Conseil d'État, la loi du 24 juillet 2015 a organisé la traçabilité de l'exécution des techniques autorisées, la centralisation par le GIC des renseignements collectés, la limitation de la durée des autorisations d'utilisation des techniques de renseignement, et également la limitation de la durée de conservation des données à compter de leur recueil.

Elle a aussi ouvert des voies de recours pour les citoyens ; un particulier peut saisir la CNCTR pour vérifier qu'aucune technique de renseignement n'a été irrégulièrement mise en œuvre à son égard (article 2 du texte et article L. 833-4 du code de la sécurité intérieure). En ce cas, la Commission procède aux vérifications nécessaires. Lorsque celles-ci sont achevées, elle informe l'auteur de la réclamation que ces vérifications ont eu lieu et qu'au terme de cette recherche, aucune irrégularité ne peut être invoquée. Cependant, la Commission ne doit ni confirmer, ni infirmer la mise en œuvre de techniques de renseignement à l'encontre du requérant ; un total de 51 réclamations a été reçu par la Commission lors de sa première année d'exercice.

De la même manière, un particulier peut saisir la Commission nationale de l'informatique et des libertés pour vérifier que ses données personnelles ne figurent pas de manière irrégulière dans un fichier concernant la sûreté de l'État ; la base légale de cette saisine est l'article 41 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; elle est rappelée dans l'article 10 de la loi relative au renseignement ; comme la CNCTR, la CNIL répond au requérant qu'elle a procédé aux vérifications demandées et qu'aucune irrégularité ne peut être invoquée ; mais elle ne peut ni confirmer, ni infirmer la

présence du nom du requérant dans un fichier relevant des services de renseignement.

Enfin, après un recours préalable devant la CNCTR, un particulier peut faire un recours devant le Conseil d'État. L'article 10 de la loi relative au renseignement crée en effet une section spécialisée au sein de cette instance pour suivre les affaires mettant en cause les techniques de renseignement soumises à autorisation sur le territoire national ou l'insertion de données personnelles dans des fichiers intéressant la sûreté de l'État (article L. 773-2 du code de justice administrative) ; depuis la création de cette section spécialisée, le Conseil d'État a été saisi par 9 requérants, dont l'un s'est désisté.

Le Conseil d'État statue, en premier et en dernier ressort, sur les recours présentés contre les autorisations individuelles de mise en œuvre des techniques de renseignement (recours en excès de pouvoir), ainsi que sur les recours présentés contre les mesures individuelles correspondant à la mise en œuvre de ces techniques ou à la mise en place des fichiers informatisés des services de renseignement (recours en plein contentieux).

Que ce soit en annulation ou en plein contentieux, le Conseil d'État statue en appliquant le principe de proportionnalité. Cette précision figure dans l'article 1er de la loi relative au renseignement. Elle est rappelée dans le dispositif de l'article L. 821-7 du code de la sécurité intérieure (techniques de renseignement susceptibles de s'appliquer à des personnalités particulièrement protégées comme les parlementaires, les magistrats, les avocats ou les journalistes pour des faits qui ne relèvent pas de leur mandat ou de leur profession) et également dans celui de l'article L. 851-3 du même code (transmission par les opérateurs de téléphonie de données de connexion recueillies au moyen d'un algorithme).

Si le Conseil d'État constate, au terme de l'examen de la requête, qu'il n'y a pas d'irrégularité dans l'autorisation ou la mise en œuvre d'une technique de renseignement ou encore dans le traitement d'un fichier, il se borne à indiquer au requérant qu'il n'y a pas d'illégalité – sans confirmer ou infirmer la mise en œuvre d'une technique de renseignement, ou encore sans révéler si le requérant se trouve ou non dans tel ou tel fichier (articles L. 773-6 et L. 773-8 du code de justice administrative).

Si le Conseil d'État constate qu'il y a une irrégularité, il annule l'autorisation – dans le cas des recours en excès de pouvoir – ou encore, outre l'annulation, il ordonne la destruction des renseignements obtenus et accorde des dommages et intérêts – dans le cas des recours en plein contentieux (article L. 773-7 du code de justice administrative).

Si le Conseil d'État constate qu'il y a une irrégularité au titre de l'article 41 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, de la même manière, il demande l'effacement des données sur le

fichier et accorde des dommages et intérêts (article L. 773-8 du code de justice administrative).

B. LA LOI DU 30 NOVEMBRE 2015

La loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales présente un certain nombre de caractéristiques.

C'est une loi qui, bien évidemment, ne vise que le territoire national ; donc, même si le dispositif concerne les communications internationales, il est indispensable, pour que le texte trouve à s'appliquer, que les communications internationales transitent par la France.

Dans le cas où l'interception des communications internationales se fait hors du territoire, la loi du 30 novembre 2015 ne s'applique pas.

La DGSE peut intercepter des flux de communications étrangères passant par la France, sous réserve de l'obtention d'une autorisation de recueil délivrée par le Premier ministre (article L. 854-2-I, premier alinéa, du code de la sécurité intérieure).

La DGSE met à disposition des autres services de renseignement concernés les flux d'informations qui ont été recueillis ; ces services peuvent alors les exploiter dans le cadre d'autorisations d'exploitation délivrées par le Premier ministre ; ces autorisations peuvent concerner les communications relatives à une zone géographique, à une organisation, à une personne ou à un groupe de personnes (article L. 854-2-III du code de la sécurité intérieure).

Les services peuvent également utiliser des données de connexion de manière non individualisée dans le cadre de certains traitements particuliers autorisés spécifiquement – par exemple des statistiques (article L. 854-2-II, premier alinéa, du code de la sécurité intérieure).

Les autorisations initiales de recueil données à la DGSE, puis les autorisations d'exploitation données aux autres services de renseignement, sont, selon la loi, accordées par le Premier ministre sans passer par la CNCTR ; toutefois, en pratique, la CNCTR délivre un avis sur ***.

Le GIC procède par voie de réquisition à l'opérateur concerné et la DGSE assure les traitements.

Dans les données recueillies, il ne doit figurer aucune communication dont les deux extrémités sont liées à un numéro d'abonnement ou à un identifiant technique rattachable au territoire national (article L. 854-1, troisième alinéa, du code de la sécurité intérieure) ; la seule exception à cette règle est constituée par les communications des personnes qui font l'objet d'interceptions de sécurité au titre de l'article L. 852-1 du code de la sécurité intérieure ou qui sont à l'étranger

et qui présentent une menace au regard des finalités de l'article L. 811-3 du code de la sécurité intérieure ; ces communications sont exploitées au GIC.

S'agissant des communications dont une extrémité est liée à un numéro d'abonnement ou à un identifiant technique rattachable au territoire national et l'autre est à l'étranger (communications mixtes), elles ne peuvent être exploitées qu'au sein du GIC.

L'ensemble de ces opérations est tracé et peut être contrôlé en permanence par la CNCTR (article L. 854-4 du code de la sécurité intérieure).

À sa demande, la CNCTR peut contrôler aussi les dispositifs techniques nécessaires à l'exécution des autorisations (article L. 854-9, premier alinéa, du code de la sécurité intérieure).

Enfin, sur sa propre initiative ou sur réclamation d'une personne souhaitant vérifier qu'aucune mesure de surveillance n'a été irrégulièrement mise en œuvre à son encontre, la CNCTR a la possibilité de s'assurer que les mesures appliquées respectent bien la loi et tout particulièrement la portée des autorisations accordées par le Premier ministre (article L. 854-9, quatrième alinéa, du code de la sécurité intérieure).

Après enquête, elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans que la mise en œuvre des mesures de surveillance soit confirmée ou infirmée (article L. 854-9, quatrième alinéa, du code de la sécurité intérieure).

Si un élément de droit ou de fait paraît irrégulier à la Commission, celle-ci adresse au Premier ministre une recommandation tendant à ce que l'irrégularité cesse et visant également à ce que les renseignements collectés soient détruits (article L. 854-9, cinquième alinéa, du code de la sécurité intérieure).

Si le Premier ministre ne donne pas suite, ou que les suites paraissent insuffisantes, le Président de la CNCTR ou trois membres de la Commission peuvent saisir le Conseil d'État (article L. 854-9, cinquième alinéa, du code de la sécurité intérieure).

C. L'EXCEPTION HERTZIENNE

Les deux lois du 24 juillet 2015 relative au renseignement et du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales ont laissé subsister une « exception hertzienne ».

Les services de renseignement, dans le domaine des ondes hertziennes (radio et télécommunications par satellite), outre des mesures globales de surveillance des réseaux, ont donc la possibilité de procéder à des interceptions, aux seules fins de défense des intérêts nationaux, sans que des autorisations

particulières ou des voies de recours spécifiques, notamment devant la CNCTR, ne soient prévues.

Il s'agit d'une disposition ancienne qui résulte 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. Cette disposition a ensuite été codifiée au sein de l'article L. 241-3 du code de la sécurité intérieure, puis elle a été transférée au nouvel article L. 811-5 de ce même code par la loi du 24 juillet 2015.

La décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016 a invalidé ce dispositif.

Le Conseil constitutionnel a en effet estimé que, faute de garanties appropriées et de précisions suffisantes sur son champ d'application – dont le domaine n'exclut pas, cependant, l'interception ou le recueil de données individualisables –, l'article L. 811-5 du code de la sécurité intérieure portait une « *atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* ».

Par ailleurs, considérant qu'une abrogation immédiate de l'article en cause 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.

En outre, le Conseil constitutionnel a 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 devaient 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 des deux lois du 24 juillet et du 30 novembre 2015.

Enfin, pour parfaire, pendant la période transitoire, le strict encadrement de la mise en œuvre des dispositions de l'article L. 811-5 du code de la sécurité intérieure, le Conseil constitutionnel a demandé que la CNCTR soit régulièrement informée sur le champ et la nature des mesures prises en application de cet article.

La CNCTR, pour sa part, a adopté une délibération, en complément de la décision du Conseil constitutionnel du 21 octobre 2016, 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. Il s'agit de la délibération n° 2/2016 du 10 novembre 2016.

Dans cette délibération, la CNCTR confirme que les mesures de surveillance hertzienne effectuées sur le territoire national doivent relever, selon les cas, de l'une ou de l'autre des deux lois de 2015 et que l'article L. 811-5 du code de la sécurité intérieure ne peut avoir pour effet de permettre aux services de

renseignement de s'affranchir des régimes d'autorisation préalable et de contrôle établis par ces deux textes.

Elle recommande au Premier ministre de demander à chacun des ministres exerçant la tutelle sur les services susceptibles de mettre en œuvre des techniques de renseignement concernant la voie hertzienne de veiller à ce qu'aucune de ces techniques ne soit mise en place sans avoir été préalablement autorisée par lui conformément à ces deux lois.

Ainsi, jusqu'au 31 décembre 2017, l'article L. 811-5 du code de la sécurité intérieure ne permet plus que des mesures générales de surveillance des réseaux, en excluant le recueil de toute donnée individualisable en dehors du cadre des lois du 24 juillet et du 30 novembre 2015.

Cette décision n'est pas sans incidence sur l'activité de certains services de renseignement, par exemple la DRM. Aujourd'hui, en effet, celle-ci procède à des interceptions de communications internationales sur le réseau hertzien (au titre de ses activités ROEM) en se servant d'antennes qui peuvent être installées sur le territoire national.

Actuellement, en vertu de la décision du Conseil constitutionnel et de la délibération de la CNCTR, les services devront – pour procéder, depuis le territoire national, à des interceptions de communications individualisées transmises par voie hertzienne – disposer d'autorisations de recueil et d'exploitation.

En matière de communications transmises par voie hertzienne, il convient cependant de distinguer plusieurs techniques qui engendrent des conséquences différentes :

– les communications relayées par satellites *** constituent, en dehors de la diffusion audiovisuelle par satellite, des communications individualisables internationales ; leur interception sur le territoire national doit donc être encadrée par la loi du 30 novembre 2015 à la suite de la décision du Conseil constitutionnel ;

– les communications radio dont la transmission s'effectue exclusivement par voie hertzienne – par émission d'un signal sans identification d'un destinataire individualisable par un opérateur de communications électroniques *** – sont des communications d'une autre nature ; leur interception sur le territoire national n'est plus encadrée par aucun dispositif légal depuis la décision du Conseil constitutionnel.

Il convient de noter que les communications dont la transmission par voie hertzienne constitue l'élongation sans fil d'un accès, soit à un opérateur (par exemple en matière de téléphonie mobile), soit à un réseau privatif (par exemple une communication wifi) ont toujours été régulées. Leur interception sur le

territoire national est encadrée par la loi du 24 juillet 2015, comme elle l'était, historiquement, par la loi du 10 juillet 1991.

Pour le premier type de communications (les communications relayées par satellites), les services de renseignement sont confrontés au défi de mettre en place, en coordination avec la CNCTR, l'ensemble des mesures requises par la loi du 30 novembre 2015 dans les délais les plus brefs.

Au total, le Gouvernement est placé aujourd'hui face à un choix :

– soit il ne propose aucun texte après le 31 décembre 2017 ; en ce cas, les interceptions hertziennes réalisées sur le territoire national sont régies, selon les cas, soit par la loi du 24 juillet 2015, soit par celle du 30 novembre 2015 ; cependant, les mesures induites par une telle assimilation (par exemple, la séparation des communications nationales et internationales, et le transfert des communications nationales vers le GIC) restent à mettre en place ; en outre, le régime de la surveillance des ondes radio reste imprécis ;

– soit le Gouvernement propose un texte ; en ce cas, en matière de communications par voie hertzienne, il devra prendre des dispositions permettant de contourner les difficultés techniques que l'on a pu voir apparaître ; par ailleurs, il pourra également réglementer les interceptions radio ; mais il devra impérativement – comme l'a d'ailleurs demandé le Conseil constitutionnel – prévoir des modes d'intervention et de contrôle qui garantissent le bon exercice des libertés publiques.

C'est cette seconde solution qui emporte l'adhésion de la DPR, étant entendu qu'il lui apparaît comme fondamental de maintenir une exception hertzienne encadrée par la loi qui garantisse la continuité de l'activité ROEM de la DRM dans la catégorie des émissions *** – émissions qui concernent essentiellement les communications institutionnelles (forces armées, gouvernements *** …).

Proposition 11. Un nouveau projet de texte doit être préparé au plus vite pour reformuler l'article L. 811-5 du code de la sécurité intérieure concernant les interceptions hertziennes. Ce texte, dont le contenu doit être déterminé en liaison avec la CNCTR, sera respectueux des libertés publiques. Pour ce faire, les mécanismes d'interception doivent être assortis de garanties réelles apportées aux personnes. Toutefois, il convient de maintenir pour la DRM une capacité de recueil d'informations dans le domaine des communications institutionnelles ***.

D. APPRÉCIATION PORTÉE SUR LES DEUX LOIS

Nous évaluerons successivement la loi du 24 juillet 2015 relative au renseignement et celle du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

1. Évaluation de la loi du 24 juillet 2015

Plusieurs indicateurs indiquent que l'application de la loi du 24 juillet 2015 répond aux objectifs attendus par le législateur.

Toutefois, il est possible de prévoir encore certaines modifications sur les dispositifs établis par ce texte. Ces modifications pourraient porter, d'une part, sur l'article L. 851-2 du code de la sécurité intérieure (recueil de données de connexion en temps réel pour les seuls besoins de la lutte antiterroriste) et, d'autre part, sur différents autres articles contenus dans ce même code, à savoir les articles L. 851-6, L. 852-1, L. 853-1, L. 853-2 et L. 853-3.

***

a. Une loi aux effets largement positifs

Six points paraissent plus particulièrement significatifs si l'on veut juger tant du caractère opérationnel que des effets fondamentalement positifs de la loi du 24 juillet 2015.

1– Tout d'abord, les décrets et les arrêtés d'application de la loi sont parus dans leur intégralité ; de la sorte, aujourd'hui, le texte est totalement applicable.

On citera le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement pris en application du livre VIII du code de la sécurité intérieure ; le décret n° 2015-1185 du 28 septembre 2015 désignant les services spécialisés de renseignement pris en application des nouveaux articles L. 811-1 et L. 853-1 à L. 853-3 du code de la sécurité intérieure ; et enfin, l'arrêté du 15 décembre 2015 modifiant l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal, pris en application de l'article 6 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

2– Ensuite, en dépit d'une certaine complexité dans la procédure en usage au sein des services avant la formulation d'une demande visant à mettre en œuvre une technique de renseignement, les dossiers émanant des différentes administrations sont désormais constitués de manière normée. En particulier, ils répondent aux prescriptions posées par l'article L. 821-2 du code de la sécurité intérieure.

3– Par ailleurs, les demandes d'utilisation des différentes techniques d'investigation ont atteint un niveau important en 2015-2016.

Les statistiques de la CNCTR indiquent en effet que l'ensemble des services de renseignement a déposé environ 66 000 demandes en 2015-2016, sur lesquelles la CNCTR a rendu 1 332 avis défavorables. Parmi les 66 000 demandes, 48 000 sont constituées par des demandes d'accès aux connexions en temps différé. En fait, il s'agit là essentiellement de demandes

préparatoires visant à obtenir les coordonnées précises de telle ou telle personne suspectée ; les demandes visant à la récupération des données de connexion *stricto sensu* sont au nombre de 15 200. Enfin, sur les 18 000 demandes restantes, les interceptions de sécurité représentent environ 8 500 demandes (principalement fondées sur la finalité de la prévention du terrorisme), la géolocalisation environ 2 100 demandes et les autres techniques de renseignement environ 7 400 demandes.

4– On enregistre une montée en puissance des demandes émanant des services du « second cercle » qui sont autorisés à recourir aux techniques de renseignement par application du décret n° 2015-1639 du 11 décembre 2015 ; ces demandes portent surtout sur la géolocalisation ; elles restent cependant nettement moins nombreuses que celles qui proviennent des services du « premier cercle ».

5– Malgré l'importance des demandes d'utilisation des techniques de renseignement, liée à l'accroissement de la menace terroriste et à l'adoption de l'état d'urgence, les dossiers sont instruits de manière très rapide. La CNCTR émet en effet un avis dans les 24 heures, ainsi que le prévoit l'article L. 821-3 du code de la sécurité intérieure.

6– Enfin, indépendamment de la CNCTR, qui, par son pouvoir de contrôle et de recommandation, constitue la principale garantie dans le cadre de la mise en œuvre des techniques de renseignement, le GIC participe, au niveau interministériel, au contrôle interne de la bonne application de la loi du 24 juillet 2015.

***

b. Une modification possible de l'article L. 851-2 du code de la sécurité intérieure

L'article L. 851-2 du code de la sécurité intérieure qui prévoit, pour les seuls besoins de la lutte antiterroriste, le recueil, auprès des opérateurs de téléphonie, des données de connexion en temps réel pourrait être modifié.

En effet, l'utilisation de cet article est très étroitement associée à celle de l'article L. 851-3 du code de la sécurité intérieure – article qui autorise, également pour les seuls besoins de la lutte antiterroriste, le recueil de données, sur les réseaux des opérateurs, en vue de révéler des comportements suspects au moyen d'un algorithme.

En fait, le système prévu par le législateur en ce domaine procède par renvois successifs.

C'est l'utilisation du système algorithmique de l'article L. 851-3 du code de la sécurité intérieure qui permet de repérer des suspects ;

***

L'algorithme est un système qui permet de déceler des comportements dangereux. Il n'a trait qu'à des données de connexion et il ne permet pas bien entendu – comme on a pu l'affirmer parfois au moment où le Parlement débattait sur la loi relative au renseignement – d'écouter directement l'ensemble des citoyens. Il permet seulement d'identifier des comportements particuliers. De la sorte, il respecte les principes fondamentaux qui régissent les libertés publiques, et, tout particulièrement, l'esprit de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés – loi que la CNCTR est également chargée d'appliquer (article 41).

Compte tenu de ces observations, la DPR préconise une modification de la rédaction de l'article L. 851-2 du code de la sécurité intérieure.

En effet, si l'on débouche, avec l'algorithme, sur des listes importantes de suspects potentiels, il ne sera plus possible de procéder par demandes individuelles pour obtenir les données de connexion. Il convient alors d'introduire dans la loi que les services de renseignement pourront également formuler leurs demandes en fournissant des listes soumises à autorisation. Par ailleurs, la durée d'autorisation pourrait également être augmentée afin que les services puissent disposer du temps nécessaire pour procéder à tous les recoupements.

Proposition 12. Procéder à une évaluation de l'application de l'article L. 851-2 du code de la sécurité intérieure concernant le recueil en temps réel des données de connexion. Apprécier l'opportunité de modifier cet article en précisant que le recueil en temps réel des données de connexion, sur les réseaux des opérateurs, s'agissant des personnes identifiées comme constituant une menace, peut être autorisé non seulement de manière individuelle mais aussi sur la base de listes fournies par les services de renseignement.

c. Autres modifications souhaitables

La pratique correspondant à la mise en œuvre des techniques de renseignement a révélé, sur certains points précis, la nécessité de prévoir une évolution de la réglementation.

L'article L. 853-2 du code de la sécurité intérieure fait une distinction entre le recueil de données informatiques (données stockées dans un système informatique) dont la durée d'autorisation est de 30 jours et la captation de données informatiques (données informatiques « vivantes » captées sous forme de flux) dont la durée d'autorisation est de deux mois. Or, en pratique, seule la technique de recueil de données informatiques est utilisée. Une « fusion » de ces deux techniques serait donc conforme à la réalité technologique. La durée d'autorisation pourrait être portée à deux mois – 30 jours étant souvent insuffisants pour la mise en œuvre effective de la technique de renseignement.

L'article L. 852-1 du code de la sécurité intérieure autorise la mise en œuvre d'une interception de sécurité à l'encontre d'une personne appartenant à

l'entourage d'un objectif répondant aux finalités de l'article L. 811-3 du même code. Cette disposition est notamment utile pour obtenir des informations au sujet de cibles recherchées dans le cadre de la prévention du terrorisme – en particulier lorsqu'elles sont présentes sur les zones djihadistes syro-irakiennes. Il serait opportun d'étendre cette notion d'entourage à la mise en œuvre du dispositif de géolocalisation prévu à l'article L. 851-4 du code de la sécurité intérieure. En effet, la géolocalisation de personnes de l'entourage d'un objectif de retour de zone de djihad sur le territoire national pour y commettre un attentat, et permettant de conduire les enquêteurs jusqu'à lui, constituerait un véritable atout pour les services de lutte antiterroriste.

L'article L. 853-3 du code de la sécurité intérieure ne prévoit l'introduction dans un lieu privé que pour un nombre limité de techniques de renseignement prévues aux articles L. 851-5 (localisation en temps réel d'une personne, d'un véhicule ou d'un objet), L. 853-1 (sonorisation et captation d'images) et L. 853-2 (recueil et captation de données informatiques). La pratique a montré que la mise en œuvre de l'article L. 851-6 (captation de données de proximité) pouvait aussi s'avérer nécessaire dans un lieu privé.

Par ailleurs, l'article L. 851-6 du code de la sécurité intérieure prévoit une durée de trois mois pour discriminer les données recueillies qui ne seraient pas en rapport avec l'autorisation délivrée. Or, l'exploitation de ces données, à la fois techniques et abstraites, peut s'avérer longue et délicate. Aussi conviendrait-il d'aménager cette période, afin de permettre aux agents des services de renseignement de pouvoir traiter efficacement l'information – sans prendre le risque de supprimer des données en rapport avec l'autorisation et qui pourraient être importantes.

Enfin, l'article L. 853-1 du code de la sécurité intérieure prévoit une durée de conservation différente pour les données obtenues, d'une part, par sonorisation et, d'autre part, par captation d'images. Or, la pratique a montré que les dispositifs vidéo intégrant un enregistrement audio ne permettaient pas de dissocier les deux types de données.

Proposition 13. Modifier certains articles du code de la sécurité intérieure afin de mettre en adéquation le cadre juridique et la réalité pratique, conformément aux analyses des pages 78 et 79 du présent rapport.

d. Les incertitudes liées à l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016

L'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 (*Tele2 Sverige AB contre Post-och telestyrelsen*) introduit des incertitudes nouvelles dans l'application de la loi du 24 juillet 2015.

Cet arrêt concerne les opérateurs de téléphonie. Leur activité est régie notamment par la directive 2002/58/CE du Parlement européen et du Conseil du

12 juillet 2002 – modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 – concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Dans le cadre de cette directive, et plus particulièrement dans le cadre de son article 15 paragraphe 1, les opérateurs européens, du fait des législations nationales, sont soumis à des obligations de conservation des données – cette conservation s'effectuant de manière généralisée et indifférenciée. C'est le cas notamment dans le droit français où l'article L. 34-1 du code des postes et des communications électroniques fixe la durée de conservation à un an.

L'intérêt de cette conservation est qu'elle permet de constituer une base de données chez chaque opérateur. C'est à partir de cette base que les juges judiciaires demandent aux opérateurs les données de connexion concernant un prévenu ou que les services de renseignement demandent à ces mêmes opérateurs l'identification de numéros de téléphone à partir d'un dossier initial concernant une personne suspecte, puis les données de connexion liées à ce numéro (48 000 demandes en 2015, y compris identification initiale des numéros d'abonnés).

Or, l'arrêt a déclaré non conforme à la Charte des droits fondamentaux de l'Union européenne cette conservation indifférenciée des données par les opérateurs, y compris lorsqu'elle est motivée par des préoccupations de sécurité publique.

L'arrêt ne remet pas en cause l'accès des juges ou des services de renseignement aux « fadettes », mais il censure leur conservation, en tout cas sur une période dépassant un délai très bref. Il n'autorise plus, au fond, que les récupérations de données de connexion effectuées en temps réel.

Cet arrêt de la Cour de justice de l'Union européenne pose donc problème. Il empiète sur la compétence des États, telle qu'elle résulte de l'application du principe de subsidiarité, et ne tient manifestement aucun compte des impératifs et des finalités qui s'attachent à l'action des services de renseignement.

Sauf inversion de jurisprudence, le Gouvernement doit exiger au plus vite auprès du Conseil la révision de la directive européenne 2002/58/CE.

2. Évaluation de la loi du 30 novembre 2015

Comme la loi du 24 juillet 2015, celle du 30 novembre 2015 a contribué à sortir de l'ombre les services de renseignement et à leur conférer une pleine reconnaissance juridique.

De la même manière, elle les a obligés aussi à recourir à des demandes d'autorisation présentées de manière normée.

Il est vrai qu'en pratique, les procédures suivies peuvent être longues. Il faut compter parfois un mois pour préparer un dossier avant de le soumettre au Premier ministre. En effet, les demandes d'autorisation transitent toujours par les plus hautes autorités des services de renseignement avant qu'elles ne soient soumises à l'appréciation de l'exécutif.

Aussi, serait-il sans doute possible de gagner du temps en simplifiant le circuit. Toutefois, à cette fin, il faudrait développer encore davantage les procédures de contrôle interne qui s'appliquent aux services.

V. RAPPORT PUBLIC DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX

*
* *

Composition de la commission de vérification des fonds spéciaux pour l'année 2016 (1)

– M. Michel Boutant, sénateur ;

– M. François-Noël Buffet, sénateur, président de la CVFS ;

– M. Jacques Myard, député ;

– M. Philipe Nauche, député.

*
* *

Instituée par l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002, la commission de vérification des fonds spéciaux (CVFS) a été profondément transformée à l'occasion de l'adoption en décembre 2013 de la loi de programmation militaire pour les années 2014 à 2019 (2).

Depuis l'entrée en vigueur en 2014 de ces nouvelles dispositions, la CVFS constitue une formation spécialisée de la délégation parlementaire au renseignement (DPR) composée de deux députés et de deux sénateurs, membres de la DPR, désignés de manière à assurer une représentation pluraliste. Son président est désigné chaque année par les membres de la délégation.

Par conséquent, la CVFS a exercé, pour la deuxième fois cette année, son contrôle sur les fonds spéciaux engagés en 2015, en application des nouvelles dispositions résultant de la loi de programmation militaire de 2013.

A. LE CADRE JURIDIQUE DU CONTRÔLE DE L'USAGE DES FONDS SPÉCIAUX

Pour des développements plus approfondis sur l'histoire des fonds spéciaux et l'évolution des modalités de leur contrôle, la commission renvoie à son rapport général publié l'an dernier au sein du rapport annuel pour 2015 de la délégation parlementaire au renseignement (3).

(1) Membres désignés lors de la réunion de la délégation parlementaire au renseignement du 14 janvier 2016.
(2) Articles 12 et 13 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
(3) Rapport n° 423 (2015-2016) relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015 fait par M. Jean-Pierre Raffarin au nom de la délégation parlementaire au renseignement.

1. Les modalités du contrôle de la CVFS

En application de l'article 154 de la loi de finances pour 2002 le but des contrôles exercés par la CVFS est de vérifier que les dépenses faites sur les fonds spéciaux [(1)] « *sont utilisés conformément à la destination qui leur a été assignée par la loi de finances* ».

L'enveloppe des fonds spéciaux votée par le Parlement dans le cadre de la loi de finances fait l'objet d'une répartition entre les différents services de renseignement et le groupement interministériel de contrôle (GIC), sur le fondement des demandes émises par ces derniers. Cette répartition, qui fait intervenir le Coordonnateur national du renseignement, est effectuée sous l'autorité du Premier ministre.

Chaque service attributaire de fonds spéciaux a pour obligation de tenir le compte d'emploi des fonds qu'il reçoit.

Pour la réalisation de ses contrôles, la commission « *prend connaissance de tous les documents, pièces et rapports susceptibles de justifier les dépenses considérées et l'emploi des fonds correspondants* » et « *se fait représenter les registres, états, journaux, décisions et toutes pièces justificatives propres à l'éclairer au cours de ses travaux de vérification* ».

Ces dispositions trouvent cependant à s'appliquer au regard de la réserve d'interprétation émise par le Conseil constitutionnel dans sa décision sur la loi de finances pour 2002 [(2)] selon laquelle les contrôles exercés par la CVFS ne sauraient « *intervenir dans la réalisation d'opérations en cours* ».

Une fois les vérifications effectuées sur un exercice budgétaire donné, la commission établit un rapport sur les conditions d'emploi des crédits, présenté aux membres de la DPR qui ne sont pas membres de la CVFS. Ce rapport « *est également remis, par le président de la délégation, aux présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances ainsi qu'au Président de la République et au Premier ministre* ».

La CVFS est également tenue de dresser un procès-verbal dans lequel elle constate que les dépenses réalisées sur les fonds spéciaux sont couvertes par des pièces justificatives pour un montant égal. Ce procès-verbal « *est remis par le président de la commission au Premier ministre et au ministre chargé du budget qui le transmet à la Cour des comptes* ».

Les travaux de la CVFS sont couverts par le secret de la défense nationale.

En pratique, le rapport de la CVFS se compose d'un procès-verbal par service attributaire d'une enveloppe de fonds spéciaux au sein duquel sont retracés

---

(1) Sur le plan budgétaire, ces crédits sont inscrits au programme n° 129 « Coordination du travail gouvernemental *» de la mission «* Direction de l'action du Gouvernement ».

(2) Décision n° 2001-456 DC du 27 décembre 2001 – Loi de finances pour 2002 (considérants 42 à 45).

les montants attribués à ce service au titre de l'exercice de l'année N-1 ainsi que leur utilisation. Les procès-verbaux, qui sont adressés aux services concernés, sont accompagnés de recommandations qui peuvent constituer des éléments de la « jurisprudence » de la commission en matière de doctrine d'emploi des fonds spéciaux et de règles de contrôle de leur usage.

Pour la première fois l'an dernier, la CVFS a souhaité, aux côtés du rapport annuel couvert par le secret de la défense nationale et dont la remise est réservée aux seules autorités définies par l'article 154 de la loi de finances pour 2002, établir un rapport public contenant des éléments d'information non protégés au titre du secret de la défense nationale.

2. Une évolution souhaitable du financement des travaux de la CVFS

En vertu du paragraphe VII *bis* de l'article 154 de la loi de finances pour 2002, les crédits nécessaires au fonctionnement de la commission sont inscrits au programme intitulé « *Coordination du travail gouvernemental* ». Les frais de mission exposés par la commission pour la réalisation de ses travaux sont donc pris en charge sur l'enveloppe budgétaire des fonds spéciaux.

Comme souligné dans le rapport de l'an dernier, la commission ne juge pas opportun que ses frais de fonctionnement continuent à être imputés sur les fonds spéciaux qu'elle contrôle. Elle appelle par conséquent de ses vœux la création d'une ligne autonome au sein des budgets des assemblées parlementaires afin de pouvoir rembourser l'exécutif des frais de fonctionnement et de mission exposés sur l'enveloppe des fonds spéciaux.

Une telle évolution nécessiterait une modification de l'article 154 de la loi de finances pour 2002.

B. ÉLÉMENTS DE RÉFLEXION SUR LA GESTION DES FONDS SPÉCIAUX EN 2015

Pour l'année 2015, le montant des fonds spéciaux affectés par la loi de finances [(1)] aux services de renseignement et au GIC s'est élevé à 50,2 millions d'euros en autorisations d'engagement et en crédits de paiement. Ces crédits sont inscrits à l'action n° 2 « *Coordination de la sécurité et de la défense* » du programme budgétaire n° 129 [(2)]. Ces crédits ont été complétés en cours d'année par des ressources additionnelles, notamment attribuées par voie de décrets de dépenses accidentelles et imprévisibles (DDAI), afin de répondre à de nouveaux besoins identifiés par les services.

Comme l'an dernier, la CVFS, dans le cadre de ses missions de contrôle conduites en 2016 sur les dépenses effectuées en 2015, a constaté que

(1) Loi n° 2014-1654 du 29 décembre 2014 de finances pour 2015.

(2) Voir page 61 du projet annuel de performance pour 2015 sur la mission « Direction de l'action du Gouvernement ».

l'emploi des fonds spéciaux répondait - à de très rares et mineures exceptions - à la doctrine qu'elle a élaborée depuis sa création, à savoir que ces crédits ne sauraient être utilisés dans un autre objectif que le financement d'activités devant obéir à des règles de confidentialité ou requérant une réactivité opérationnelle incompatible avec les règles de la comptabilité publique.

Dans un contexte de revalorisation substantielle des moyens humains et budgétaires accordés aux services de renseignement [(1)], notamment en réponse à la menace terroriste sans précédent à laquelle est exposé notre pays, **la CVFS continue à plaider en faveur d'une augmentation substantielle du montant de ces crédits**. Une telle évolution apparaîtrait cohérente avec l'activité opérationnelle soutenue à laquelle sont aujourd'hui confrontés les services de renseignement et permettrait également de limiter le recours à l'octroi de ressources additionnelles en cours d'année.

À cet égard, la commission ne saurait que renouveler ses remarques sur la nécessité de ne recourir aux ressources additionnelles, en particulier par la voie de DDAI, que pour le financement d'activités ponctuelles n'ayant pas vocation à s'inscrire dans la durée. À nouveau, la CVFS a en effet constaté le recours à des DDAI pour financer, au-delà du déclenchement de la crise, des dépenses qui, avec le temps, deviennent prévisibles. Une telle pratique est discutable puisque l'usage des DDAI constitue un cercle vicieux dans la mesure où la crise dure généralement plus longtemps que le décret ; de telle sorte que les services doivent intégrer dans leur dotation initiale en fonds spéciaux de nouvelles dépenses qui supposent des économies parfois préjudiciables à la conduite de leurs autres missions.

Par conséquent, une revalorisation substantielle de la dotation en fonds spéciaux offrira aux services concernés une gestion plus saine et sereine de leurs budgets sur le moyen terme et sera de nature à restreindre le recours aux DDAI à son objet principal : la gestion temporaire de l'imprévisible. À cet égard, la commission note avec satisfaction l'inscription en loi de finances initiale pour 2017 d'un montant de fonds spéciaux de 67,8 millions d'euros en autorisations d'engagement et en crédits de paiement.

Par ailleurs, comme souligné l'an dernier dans le rapport public de la commission, la revalorisation de l'enveloppe, outre qu'elle sera de nature à limiter le recours aux ressources additionnelles, pourra venir en soutien « *d'une politique ambitieuse et proactive conduite par les services afin de répondre à leurs missions, d'entraver les menaces qui pèsent sur notre pays et d'anticiper celles qui pourraient survenir dans les prochaines années* ».

Enfin, la commission renouvelle son constat effectué l'an dernier, selon lequel les fonds spéciaux font l'objet d'une gestion rigoureuse de la part des services, et adresse ses félicitations à l'attention des agents qui sont chargés de ces

(1) En particulier en application du plan de lutte antiterroriste (PLAT) de janvier 2015 et du pacte de sécurité (PDS) de novembre 2015.

fonctions pour leur implication personnelle, leur professionnalisme et leur sens du devoir. Elle continue cependant à plaider en faveur de la promotion d'une nomenclature unique des pièces justificatives et des modes de comptabilité afin de faciliter ses contrôles et d'unifier les méthodes de gestion interne. Cette évolution pourrait être favorisée par un travail conduit par le Coordonnateur national du renseignement qui pourrait diffuser les bonnes pratiques et y sensibiliser les acteurs (y compris par la diffusion d'une directive s'inspirant des préconisations de la commission).

CONCLUSION GÉNÉRALE

Face à des menaces multiples dont on perçoit la durée et l'intensité, la France a renforcé ses services de renseignement, consolidé ses dispositifs législatifs et réglementaires, et agi, dans le cadre européen, pour que ses partenaires œuvrent dans la même direction et que les normes européennes intègrent de nouvelles exigences relatives à la protection des citoyens, ce qui constitue le socle permettant l'exercice des libertés publiques et la garantie de préservation de leur vie privée.

Dans cette période troublée et à la veille du départ annoncé de plusieurs directeurs des services, les perspectives des prochaines échéances électorales constituent une période propice à la mise en avant de projets de réformes plus ou moins ambitieuses des services de renseignement. La Délégation considère que, si la politique de renseignement ne doit pas être tenue à l'écart du débat, elle doit être traitée avec une éthique de responsabilité et être préservée des effets de communication et des enjeux de pouvoirs ou de personnes.

Il appartiendra aux autorités de l'État issues des prochaines élections d'orienter la politique publique du renseignement, de conduire d'éventuelles réformes et de nommer de nouveaux dirigeants.

La Délégation considère que ces décisions devront être prises à l'aune de la seule préoccupation de la préservation d'un équilibre optimal entre la protection des libertés publiques et de la vie privée de nos concitoyens qui constitue le socle de nos valeurs et le renforcement de l'efficacité des services de renseignement dont l'importance est stratégique pour préserver notre souveraineté nationale et protéger nos concitoyens.

Elle continuera pour sa part à veiller à la préservation de cet équilibre et au développement de nos capacités de renseignement dans un monde que l'on perçoit comme plus incertain et plus dangereux.

LISTE DES PROPOSITIONS

Proposition 1. La DPR souhaite que la transposition de la directive du 21 avril 2016 sur le PNR européen soit effectuée par les pays membres le plus rapidement possible. Elle demande à la France d'accélérer cette transposition dans le droit national et à ses représentants auprès des différents gouvernements de l'Union européenne d'agir auprès d'eux pour qu'ils aillent dans le même sens. Elle note également que la directive présente certaines limites et elle suggère qu'une réflexion puisse être conduite pour renforcer encore l'efficacité du texte.

Proposition 2. La DPR demande la remise du rapport annuel de synthèse des crédits de l'année précédente au plus tard le 1er avril de l'année en cours ; pour le cas où ce rapport ne pourrait être remis qu'à l'automne, elle demande que le document comporte également l'exécution des crédits de l'exercice en cours et une présentation des crédits inscrits dans le projet de loi de finances pour l'année à venir ; enfin, la DPR souhaite que le rapport annuel d'activité des services portant sur l'année précédente lui soit présenté avant le 30 juin de l'année en cours.

Proposition 3. La DPR réitère sa demande de transformer le poste de Secrétaire général de l'ISR en un poste de chef de service, chargé de l'encadrement et du suivi des inspecteurs des services de renseignement.

Proposition 4. Poursuivre, malgré les difficultés budgétaires, les recrutements au sein des services de renseignement**,** ainsi que le renforcement de leurs moyens matériels et humains.

Proposition 5. Il serait souhaitable que le Commissaire à l'information stratégique et à la sécurité économiques puisse définir les bases juridiques nécessaires à la création d'une organisation référente en matière de conformité anti-corruption ; cette structure servirait de conseil aux entreprises entretenant des relations commerciales soutenues avec l'étranger.

Proposition 6. Intégrer dans les études conduites par le Commissaire à l'information stratégique et à la sécurité économiques la question des objets connectés, afin qu'il prépare une réglementation propre à ces objets.

Proposition 7. Réfléchir à une nouvelle implantation mieux adaptée pour le siège de la DGSI et accélérer les recrutements au sein des échelons départementaux et régionaux de ce service.

Proposition 8. Après la finalisation du cadre juridique, les moyens humains et matériels dédiés au renseignement pénitentiaire doivent poursuivre leur montée en puissance au cours des années à venir. La Délégation parlementaire au renseignement accordera une attention particulière à la mise en œuvre de la réforme au cours de l'année à venir.

Proposition 9. Il convient de confier à l'ISR une étude portant sur les questions liées aux recrutements, aux rémunérations et aux carrières des personnels des services de renseignement.

Proposition 10. Il serait souhaitable que l'ISR réalise une étude sur les différents fichiers des services de renseignement, portant notamment sur leur organisation et sur leur coordination.

Proposition 11. Un nouveau projet de texte doit être préparé au plus vite pour reformuler l'article L. 811-5 du code de la sécurité intérieure concernant les interceptions hertziennes. Ce texte, dont le contenu doit être déterminé en liaison avec la CNCTR, sera respectueux des libertés publiques. Pour ce faire, les mécanismes d'interception doivent être assortis de garanties réelles apportées aux personnes. Toutefois, il convient de maintenir pour la DRM une capacité de recueil d'informations dans le domaine des communications institutionnelles ***.

Proposition 12. Procéder à une évaluation de l'application de l'article L. 851-2 du code de la sécurité intérieure concernant le recueil en temps réel des données de connexion. Apprécier l'opportunité de modifier cet article en précisant que le recueil en temps réel des données de connexion, sur les réseaux des opérateurs, s'agissant des personnes identifiées comme constituant une menace, peut être autorisé non seulement de manière individuelle mais aussi sur la base de listes fournies par les services de renseignement.

Proposition 13. Modifier certains articles du code de la sécurité intérieure afin de mettre en adéquation le cadre juridique et la réalité pratique, conformément aux analyses des pages 78 et 79 du présent rapport.

EXAMEN PAR LA DÉLÉGATION

Réunie le jeudi 2 mars 2017 sous la présidence de Mme Patricia Adam, présidente, la Délégation a procédé à l'examen du rapport annuel. Après un exposé de sa présidente, la Délégation a adopté son rapport pour 2016 (chapitres 1 à 4), en application du VI de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958.

Par ailleurs, elle avait entendu, le jeudi 12 janvier 2017, la présentation du rapport de la Commission de vérification des fonds spéciaux en application du VI de l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002 (chapitre 5).