

N° 3524

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale

le 25 février 2016

N° 423

SÉNAT

SESSION ORDINAIRE DE 2015-2016

Enregistré à la Présidence du Sénat

le 25 février 2016

DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

RAPPORT

relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015

Par

M. Jean-Pierre RAFFARIN,

Sénateur

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

Premier vice-présidente de la délégation.

Déposé sur le Bureau du Sénat
par M. Jean-Pierre RAFFARIN

Président de la délégation.

SOMMAIRE

	<u>Pages</u>
AVANT-PROPOS	9
INTRODUCTION	11
CHAPITRE PREMIER : LES ACTIVITÉS DE LA DPR AU COURS DE L'ANNÉE ÉCOULÉE	15
I. LES TRAVAUX CONDUITS PAR LA DÉLÉGATION EN 2015	15
II. LES INNOVATIONS INTRODUITES PAR LA LOI RELATIVE AU RENSEIGNEMENT	18
III. LE SUIVI DES PROPOSITIONS DE LA DÉLÉGATION	19
A. LA LUTTE CONTRE LA MENACE TERRORISTE	19
B. L'ORGANISATION DU RENSEIGNEMENT INTÉRIEUR	21
C. LA GESTION DES RESSOURCES HUMAINES	22
D. LE RENSEIGNEMENT ÉCONOMIQUE ET FINANCIER	24
CHAPITRE II - LA MISE EN ŒUVRE PROGRESSIVE DE LA LOI SUR LE RENSEIGNEMENT	27
I. UNE LOI LARGEMENT INSPIRÉE DES TRAVAUX DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT	27
A. LA REPRISE PAR LA LOI DU 24 JUILLET 2015 DE L'ESSENTIEL DES PRÉCONISATIONS FORMULÉES EN 2014	27
1. <i>Le choix d'un cadre d'action des agents, pour des finalités précisées</i>	27
2. <i>Le renforcement des garanties des citoyens</i>	28
3. <i>L'attribution de techniques nouvelles, pour certaines inspirées des techniques applicables en police judiciaire</i>	29
4. <i>Le maintien de la centralisation des éléments collectés</i>	30
5. <i>Le choix d'une structure aux moyens et aux pouvoirs adaptés aux nouveaux enjeux du contrôle</i>	30
6. <i>L'extension des pouvoirs de contrôle de la DPR</i>	31
B. LE CHOIX CONTESTABLE DE NE PAS AVOIR PARACHEVÉ LE SYSTÈME PAR UN RENFORCEMENT SUBSTANTIEL DE L'INSPECTION DES SERVICES DE RENSEIGNEMENT	31
C. LE REFUS D'UNE EXTENSION DES POUVOIRS DE LA CNCTR EN MATIÈRE DE CONTRÔLE DES FICHIERS	31
II. UNE MONTÉE EN PUISSANCE PROGRESSIVE DES ACTEURS DU CONTRÔLE	32

A. LA MISE EN PLACE DE LA CNCTR, EN PHASE DE MONTÉE EN PUISSANCE.....	32
1. <i>Le maintien et le renforcement des moyens de contrôle de la CNCIS</i>	32
2. <i>Une montée en puissance progressive des moyens de la CNCTR</i>	33
3. <i>Le constat d'importantes différences par rapport à la CNCIS</i>	34
a) <i>La collégialité</i>	34
b) <i>La pression inédite d'un contrôle juridictionnel</i>	35
B. LE SOUS-DIMENSIONNEMENT DU GROUPEMENT INTER-MINISTÉRIEL DE CONTRÔLE (GIC) POUR RÉPONDRE AUX DÉFIS POSÉS PAR LA LOI DU 24 JUILLET 2015.....	35
1. <i>Le positionnement ambigu du GIC, à l'organisation perfectible</i>	35
2. <i>Le développement attendu d'une application informatique permettant de centraliser effectivement les demandes</i>	36
C. UNE DEMANDE DE MISE EN ŒUVRE DE NOUVELLES TECHNIQUES ENCORE RELATIVEMENT FAIBLE.....	37
1. <i>Une augmentation des demandes difficile à évaluer préalablement</i>	37
2. <i>La prudence de la DGSI dans la mise en œuvre des techniques nouvelles ?</i>	38
D. LA PUBLICATION DES DÉCRETS D'APPLICATION.....	38
III. LE DÉFI D'UN CONTRÔLE EFFECTIF DE LA MISE EN ŒUVRE DES NOUVELLES TECHNIQUES DE RENSEIGNEMENT	38
A. LES DIFFICULTÉS D'ÉTENDRE LE SCHÉMA APPLICABLE AUX TECHNIQUES PERMISES PAR LA LOI DU 20 JUILLET 1991 À CERTAINES TECHNIQUES NOUVELLES DE RENSEIGNEMENT	38
B. UNE DÉSIGNATION TRÈS LARGE DES SERVICES POUVANT BÉNÉFICIER DE TECHNIQUES DU RENSEIGNEMENT COMPLIQUANT LE CONTRÔLE DE LA MISE EN ŒUVRE DES TECHNIQUES DE RENSEIGNEMENT	39
1. <i>Une désignation extensive des services autorisés à recourir aux techniques de renseignement</i>	39
2. <i>Le risque d'un contournement des procédures applicables dans un cadre judiciaire</i>	40
3. <i>Le risque d'affecter l'efficacité des services de renseignement du premier cercle</i>	41
4. <i>Les effets mécaniques d'une telle extension sur les organes de traitement (GIC) ou de contrôle (CNCTR)</i>	42
C. LA NÉCESSITÉ DE METTRE EN PLACE DES PROCÉDURES DE CONTRÔLES COMPLÉMENTAIRES POUR S'ASSURER DU RESPECT DES DISPOSITIONS LÉGALES APPLICABLES	43
1. <i>L'audit interne : un dispositif nécessaire mais insuffisant sans un audit externe robuste et permanent des procédures</i>	43
a) <i>Un contrôle interne rendu indispensable par la collecte décentralisée des renseignements</i>	43
b) <i>La nécessité d'un contrôle interne robuste et standardisé au sein des services du « deuxième cercle »</i>	44
2. <i>La mise en place d'une inspection des services de renseignement pérenne pour permettre un audit régulier du contrôle interne</i>	44
IV. LES PROPOSITIONS DE LA DPR	45
CHAPITRE III : LA SURVEILLANCE INTERNATIONALE	47

I. LA SURVEILLANCE INTERNATIONALE A L'ÉPREUVE DE L'ORGANISATION	47
A. UN SERVICE SPÉCIALISÉ DANS LE RENSEIGNEMENT EXTÉRIEUR : LA DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE (DGSE)	48
1. <i>Statut</i>	48
2. <i>Missions</i>	48
3. <i>Organisation</i>	49
4. <i>Ressources humaines</i>	49
5. <i>Moyens budgétaires</i>	49
B. UN SERVICE SPÉCIALISÉ DANS LE RENSEIGNEMENT MILITAIRE : LA DIRECTION DU RENSEIGNEMENT MILITAIRE (DRM)	50
1. <i>Statut</i>	50
2. <i>Missions</i>	50
3. <i>Organisation</i>	51
4. <i>Ressources humaines</i>	52
5. <i>Moyens budgétaires</i>	52
C. LES QUATRE AUTRES SERVICES SPÉCIALISÉS ONT DES ACTIVITÉS INTERNATIONALES PLUS RÉDUITES	52
1. <i>La DNRED</i>	52
2. <i>TRACFIN</i>	53
3. <i>La DPSD</i>	53
4. <i>La DGSJ</i>	54
D. LE CHOIX DE LA SPÉCIALISATION ET DE LA MUTUALISATION	54
II. LA SURVEILLANCE INTERNATIONALE À L'ÉPREUVE DES TECHNOLOGIES	55
A. LA SURVEILLANCE DES COMMUNICATIONS (RENSEIGNEMENT D'ORIGINE ÉLECTROMAGNÉTIQUE - ROEM)	56
B. L'OBSERVATION (SATELLITES, AVIONS, DRONES, NAVIRES)	57
1. <i>Les satellites d'observation</i>	57
a) Les moyens actuels	57
b) Les moyens futurs	57
2. <i>Les aéronefs</i>	59
a) Les avions de surveillance et de reconnaissance	59
b) Les capteurs embarqués sur des aéronefs de combat et de patrouille maritime	59
c) Les capteurs embarqués sur les drones	59
d) Le traitement automatisé des images.....	60
C. LE RENSEIGNEMENT HUMAIN	60
1. <i>La DRM</i>	60
a) Les capacités propres de la DRM.....	60
b) L'administration de l'ensemble des sources humaines des armées	60
c) La centralisation et l'enrichissement du renseignement	61
2. <i>La DGSE</i>	62
a) Mission de la direction du renseignement.....	62
b) Moyens de la direction du renseignement.....	62
c) Organisation.....	62
D. LE CYBER, UN ESPACE SPÉCIFIQUE	62

E. LE RENSEIGNEMENT PARTENARIAL	63
III. LA SURVEILLANCE INTERNATIONALE A L'ÉPREUVE DU DROIT	63
A. LES COMMUNICATIONS ÉLECTRONIQUES INTERNATIONALES UTILISANT LES RÉSEAUX PHYSIQUES.....	63
1. La nécessité de placer la surveillance dans un cadre légal de niveau législatif.....	63
2. L'insertion de dispositions dans le projet de loi relative au renseignement	64
3. Ces dispositions ont été jugés insuffisantes par le Conseil constitutionnel	65
4. L'obligation de préciser et de compléter le dispositif envisagé par une loi spécifique relative aux mesures de surveillance des communications électroniques internationales	65
5. Le nouveau cadre légal de la surveillance des communications électroniques internationales	67
6. Hors territoire national.....	70
B. LES COMMUNICATIONS ÉLECTRONIQUES INTERNATIONALES PAR VOIES HERTZIENNES.....	71
IV. LA SURVEILLANCE INTERNATIONALE À L'ÉPREUVE DU TERRORISME	73
A. UNE FORME NOUVELLE DE MENACE : FURTIVE, CHANGEANTE, ÉVOLUTIVE.....	74
1. Il s'agit d'une menace hybride.....	74
2. Il s'agit d'une menace autoreproductrice	74
3. Il s'agit d'une menace matérielle et immatérielle	75
4. Il s'agit d'une menace furtive	75
5. Il s'agit d'une menace capable de mener des actions terroristes dans le monde entier	75
6. Il s'agit d'une menace de forte intensité	75
B. UN IMPACT SUR L'ORGANISATION DE LA SURVEILLANCE INTERNATIONALE	76
1. L'indispensable coopération interservices	76
a) La coopération dans l'emploi des capteurs.....	77
b) La mise en place de cellule inter-agences	77
2. La complexe problématique européenne	78
a) L'institution d'un coordonnateur pour la lutte contre le terrorisme.....	78
b) La sous-utilisation du Système d'information Schengen (SIS)	79
c) Le laborieux aboutissement du PNR	80
d) Une avancée en matière de système spatial d'observation	82
3. La coopération internationale entre services	82
4. La concentration des efforts ne doit pas se faire au détriment des autres missions qui demeurent stratégiques.....	83
5. Une problématique qui dépasse la seule action des services de renseignement et la seule réponse militaire.....	83
V. LES PROPOSITIONS DE LA DPR.....	85
CHAPITRE IV L'ÉVALUATION DE LA POLITIQUE PUBLIQUE DE RENSEIGNEMENT.....	87
I. LES APPORTS DE LA LOI DU 24 JUILLET 2015 RELATIVE AU RENSEIGNEMENT	87
A. LA DÉFINITION D'UNE POLITIQUE PUBLIQUE DU RENSEIGNEMENT	88

B. LES MOYENS D'INFORMATION DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT COMPLÉTÉS	89
1. Les documents communiqués à la DPR	89
2. Une extension de la liste des personnes susceptibles d'être entendues par la DPR.....	91
II. UNE MISE EN ŒUVRE ENCORE TIMIDE	92
A. LA STRATÉGIE NATIONALE DU RENSEIGNEMENT ET LE PLAN NATIONAL D'ORIENTATION DU RENSEIGNEMENT	92
B. LE RAPPORT ANNUEL DE SYNTHÈSE DES CRÉDITS CONSACRÉS AU RENSEIGNEMENT.....	93
C. LE RAPPORT ANNUEL D'ACTIVITÉ ET L'ORGANISATION DES SERVICES DE RENSEIGNEMENT.....	96
III. LES PROPOSITIONS DE LA DPR	100
CHAPITRE 5 : LE RAPPORT GÉNÉRAL DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX.....	101
INTRODUCTION.....	102
I. LE CONTRÔLE DES FONDS SPÉCIAUX OU LA LONGUE MARCHÉ DU PARLEMENTARISME	104
A. QUAND L'ÉTAT SECRET EST AUSSI UN ÉTAT DE DROIT	104
1. Une tradition monarchique revivifiée mais rectifiée par la Quatrième République	104
2. La CVFS : un contrôle parlementaire né d'une polémique (2001).....	106
3. Le contrôle des fonds spéciaux comme amplification des activités de la délégation parlementaire au renseignement (2013)	110
B. LA QUESTION DES « OPÉRATIONS EN COURS » OU LA CADUCITÉ DE LA DÉCISION DE 2001.....	115
C. QUELS MOYENS POUR LE CONTRÔLE DES FONDS SPÉCIAUX ? UNE NÉCESSAIRE RÉVISION LÉGISLATIVE.....	117
II. ÉLÉMENTS DE SYNTHÈSE PUBLIQUE EXTRAITS DES PROCÈS-VERBAUX.....	123
A. POUR UNE REVALORISATION DU BUDGET DES FONDS SPÉCIAUX	123
B. POUR UN USAGE RATIONALISÉ DES FONDS SPÉCIAUX.....	123
C. LA QUESTION DES DDAI	125
D. REVOIR LES MÉCANISMES D'ATTRIBUTION DES FONDS SPÉCIAUX	126
E. VERS UNE STANDARDISATION DE LA GESTION DES FONDS SPÉCIAUX.....	127
CONCLUSION	128
RELEVÉ DES RECOMMANDATIONS DE LA CVFS.....	129
EXAMEN PAR LA DÉLÉGATION	131

LES PROPOSITIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT	132
I. PROPOSITIONS CONCERNANT LA MISE EN ŒUVRE DE LA LOI SUR LE RENSEIGNEMENT	132
II. PROPOSITIONS RELATIVES À LA SURVEILLANCE INTERNATIONALE	133
III. PROPOSITIONS RELATIVES À L'ÉVALUATION DE LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT	134
ANNEXE 1	135
ANNEXE 2	137
ANNEXE 3	144
ANNEXE 4	145
ANNEXE 5	146
ANNEXE 6	148
ANNEXE 7	150

AVANT-PROPOS

POUR UNE ÉVALUATION PERFORMANTE DE LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

2015 est une année sombre, celle d'une France endeuillée par trois attentats terroristes meurtriers qui s'inscrivent dans une suite ininterrompue, conséquence de l'émergence du djihadisme radical.

L'intensité de ces attaques marque une étape nouvelle.

Malgré les efforts de nos services de renseignement pour déjouer ou entraver ces attaques, leur survenance même questionne naturellement leur efficacité.

Paradoxalement, 2015 est aussi l'année au cours de laquelle le Parlement s'est appliqué, pour la première fois, à accompagner la montée en puissance des services de renseignement, autorisés à utiliser des techniques nouvelles plus intrusives, par l'élaboration d'un cadre juridique plus solide afin de sécuriser leurs actions, mais aussi et surtout, de définir des procédures protectrices des libertés et de la vie privée de nos concitoyens. Deux lois ont été adoptées en ce sens aux termes de débats nourris, à l'Assemblée nationale comme au Sénat, mais aussi dans l'opinion publique et dans les médias. Pour répondre à l'évolution de la menace terroriste, les services de renseignement ont vu également leurs moyens renforcés, en effectifs, en fonctionnement et en équipement.

Il conviendra d'analyser et d'évaluer comment ces services ont répondu à la menace et comment ils ont mis en œuvre les nouveaux moyens qui leur ont été accordés.

Si la délégation parlementaire au renseignement a été régulièrement informée de l'évolution des menaces et des réponses apportées par les services pour faire face, elle ne pouvait objectivement, sans entrer dans un contrôle opérationnel, procéder à une évaluation formative de l'efficacité de la politique de renseignement face à la menace terroriste. Elle sera en revanche certainement appelée à réaliser, en 2016, une évaluation *ex post* sur la base des retours d'expérience, le déroulement des enquêtes étant susceptible de révéler des points de force et de faiblesse ainsi que des axes d'amélioration.

La délégation peut néanmoins confirmer, au terme de ses travaux, que la menace terroriste est inscrite dans la durée et que les attaques sont susceptibles de croître en fréquence comme en intensité.

La politique publique du renseignement devra, en conséquence, se placer dans cette perspective. Cette profondeur temporelle implique une vision stratégique renouvelée et, probablement, de la continuité dans le renforcement des moyens amorcé en 2015.

Une politique publique, porteuse d'enjeux aussi lourds, s'appuyant sur des moyens en croissance, ne peut être conduite sans un appareil d'évaluation plus robuste. Cette évaluation doit s'ancrer sur une méthodologie cohérente, reposant d'une part, sur le renforcement du contrôle interne au sein des services de renseignement mais aussi, d'autre part, sur la mise en place d'un véritable service interministériel d'inspection des services de renseignement, structuré, pérenne, doté d'un encadrement permanent, capable de réaliser, en temps et en heure, des missions de contrôle et d'étude au profit de l'exécutif, mais aussi de la DPR. Sans cela, l'exécutif sera dépourvu d'instruments d'analyse solide de la performance des services dont il est le garant, et le Parlement, d'éléments d'appréciation objectifs et sérieux. Sans cela, le débat sur l'efficacité des services risque de se réduire à de vaines et stériles polémiques. Telle est la principale conclusion de ce rapport.

INTRODUCTION

2015, constituera une étape importante pour la politique publique du renseignement.

Pour la première fois, la France s'est dotée d'un cadre législatif complet autorisant et encadrant l'usage par les services spécialisés, de techniques de renseignement, en adoptant deux lois, la première **n° 2015-912 du 24 juillet 2015 relative au renseignement**, la seconde **n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales**. Ces deux lois à la préparation desquelles la délégation parlementaire au renseignement a été étroitement associée, établissent un équilibre entre l'indispensable protection des droits et de la vie privée garantie par la Constitution et la nécessaire protection de la sécurité de nos concitoyens et des intérêts fondamentaux de la Nation, à laquelle contribue par leurs capacités opérationnelles de haut niveau, les services spécialisés de renseignement.

Dans le même temps, la menace terroriste, dont l'intensité n'a fait que croître à raison du développement de réseaux djihadistes, notamment Daech, qui ont développé leurs activités dans des zones instables en Irak et en Syrie, au Yémen, dans la bande sahélo-saharienne et en Libye et qui ont été rejoints par un nombre considérable de combattants étrangers dont un nombre significatif originaires de notre pays et de pays voisins, s'est concrétisée par plusieurs attaques meurtrières d'envergure sur le territoire national, notamment les 7, 8 et 9 janvier puis le 13 novembre, sans compter les opérations qui ont pu être déjouées et/ou entravées.

L'activité de la délégation parlementaire au renseignement au cours de cette année s'est donc très naturellement focalisée sur le travail législatif et les modalités de mise en œuvre de la loi, sur la montée en puissance des services de renseignement qui se sont vus affectés de nouveaux moyens et sur le développement de leur coopération dans la lutte contre le terrorisme.

La délégation n'en a pas moins poursuivi son travail de fond en appréciant la mise en œuvre des recommandations qu'elle avait formulées dans son précédent rapport, notamment dans le domaine du renseignement économique et financier et en entamant une réflexion méthodologique sur les modalités et outils à développer pour assurer la mission d'évaluation de la politique publique du renseignement telle qu'elle a été redéfinie par 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**

Il importe en effet que le Président de la République, le Premier ministre et les présidents des assemblées parlementaires, auxquels est destiné ce travail, puissent prendre connaissance de recommandations et d'observations fondées sur une analyse de l'action du Gouvernement et de sa mise en œuvre par les services spécialisés et les organes qui, au sein des administrations de l'État, contribuent à la politique publique du renseignement.

Il importe également à travers ce rapport public que la délégation parlementaire au renseignement puisse apporter, à la représentation nationale et à l'ensemble de nos concitoyens, des éléments d'appréciation sur la place et le rôle des administrations publiques en charge de cette mission stratégique, participant ainsi à l'émergence d'une culture du renseignement et permettant une appréhension plus réaliste et plus objective de leurs missions.

Naturellement, certaines informations portées à la connaissance des membres de la DPR ne peuvent, pour des raisons de sécurité, être rendues publiques sous peine d'accroître la vulnérabilité de notre pays aux actions de ses rivaux et adversaires. Comme dans son précédent rapport, la délégation a choisi de masquer les passages sensibles, couverts par le secret de la défense nationale, au moyen d'un signe typographique ***, invariable quelle que soit l'ampleur des informations rendues ainsi illisibles.

Ce rapport comporte quatre chapitres :

Le premier est un compte-rendu de son activité et de la mise en œuvre des recommandations de son rapport pour 2014.

Le deuxième qui porte sur la mise en œuvre de la loi relative au renseignement, aborde à la fois la publication des textes réglementaires d'application, la mise en place et les moyens affectés à la CNCTR ainsi que les premiers mois d'exercice de son activité, enfin la place nouvelle qu'occupe désormais le groupement interministériel de contrôle dans le dispositif d'autorisation, de conservation des données et de traçabilité mis en œuvre ainsi que le renforcement de ses moyens juridiques, techniques et humains.

Le troisième chapitre développe le cadre d'organisation de la surveillance internationale, les moyens qui lui sont affectés, le cadre juridique dans lequel elle s'exerce et son adaptation aux évolutions des menaces, notamment celles du terrorisme.

Enfin, le quatrième chapitre rassemble les premiers éléments d'une réflexion sur l'évaluation de la politique publique du renseignement dont la mission est confiée à la DPR, sur la pertinence des outils dont elle dispose pour réaliser ses travaux et la méthodologie dont elle devra se doter dans les prochaines années pour les améliorer. Sans doute, l'exigence de la réussite qui ne souffre aucun faux-pas et la difficulté de communication de façon explicite sur les résultats obtenus, rendent-elles ce travail difficile mais il

n'en est pas moins nécessaire de disposer d'indicateurs pour mesurer l'activité des services et l'amélioration de leur performance.

Par ailleurs, ce document parlementaire comprend, au chapitre 5, sous sa responsabilité, le rapport général de la Commission de vérification des fonds spéciaux, présenté aux autres membres la délégation parlementaire au renseignement, le 14 janvier 2016, en application du VI de l'article 154 de la loi de finances pour 2002 modifié.

La prise de conscience de l'importance, pour le devenir de notre modèle républicain et démocratique de société, de la fonction de connaissance et d'anticipation et du rôle spécifique des services de renseignement pour réduire les incertitudes, déjouer et entraver l'action de ceux qui le menacent et éclairer la décision de nos dirigeants, mais aussi la crainte toujours sous-jacente que la revalorisation nécessaire de leur cadre d'action, si elle n'est pas régulée de façon appropriée, puisse porter atteinte aux libertés et à la vie privée, alimenteront de façon croissante le débat public. La responsabilité du législateur qui délimite le cadre de la politique publique du renseignement, du Gouvernement qui en conduit la mise en œuvre et de ceux qui en contrôlent l'exécution qu'il s'agisse de services d'inspection, d'autorités administratives indépendantes, de juridictions ou de la délégation parlementaire, mais aussi de ceux, universitaires, journalistes, experts qui la commentent, est immense pour tout à la fois maintenir l'efficacité opérationnelle et garantir le respect des valeurs fondatrices du contrat social.

La délégation parlementaire au renseignement souhaite présenter une appréciation aussi objective que possible forgée par les auditions, la prise de connaissance de documents, des visites au sein des services et organisations et l'expérience acquise de la mission de contrôle. Ses membres sont conscients de l'enjeu cette mission et de l'exigence de responsabilité qui doit en permanence, au-delà de la légitimité qui leur est conférée par la loi et par leur mandat parlementaire, les guider dans son accomplissement. Cette éthique est encore plus nécessaire lorsque notre pays est victime d'attaques terroristes sur son territoire et doit assurer la protection de sa population.

Réunies le jeudi 14 janvier 2016 sous la présidence de M. Jean-Pierre Raffarin, président, la délégation parlementaire a adopté le présent rapport relatif à son activité pour l'année 2015.

CHAPITRE PREMIER : LES ACTIVITÉS DE LA DPR AU COURS DE L'ANNÉE ÉCOULÉE

La composition de la délégation parlementaire au renseignement, au cours de l'année 2015, était la suivante :

- Pour l'Assemblée nationale :

Mme Patricia Adam, députée Socialiste, républicain et citoyen, *première vice-présidente de la délégation*, présidente de la commission de la Défense nationale et des forces armées

M. Jean-Jacques Urvoas, député, Socialiste, républicain et citoyen, président de la commission des Lois ;

M. Jacques Myard, député, Les Républicains, désigné par le président de l'Assemblée nationale ;

M. Philippe Nauche, député Socialiste, républicain et citoyen, désigné par le président de l'Assemblée nationale.

- Pour le Sénat :

M. Philippe Bas, sénateur Les Républicains, président de la commission des Lois du Sénat ;

M. Jean Pierre Raffarin, sénateur Les Républicains, *président de la délégation*, président de la commission des Affaires étrangères et de la Défense du Sénat ;

M. Michel Boutant, sénateur socialiste et républicain, *deuxième vice-président de la délégation*, désigné par le président du Sénat ;

M. Jean-Patrick Courtois, sénateur Les Républicains, puis M. François-Noël Buffet, sénateur Les Républicains, désigné par le président du Sénat.

I. LES TRAVAUX CONDUITS PAR LA DÉLÉGATION EN 2015

Au cours de l'année, la délégation parlementaire au renseignement s'est réunie à quatorze reprises.

La délégation a d'abord provoqué deux réunions extraordinaires, à la suite des événements tragiques des mois de janvier et novembre 2015, pour entendre les premières explications des services en charge du renseignement intérieur et du renseignement extérieur, ainsi que leurs autorités de tutelle : réunions des 22 janvier et 26 novembre (*voir en annexe 1 le communiqué de presse du 26 novembre*).

Outre deux réunions de travail consacrées à son organisation interne, elle a procédé à de nombreuses auditions, conformément à ses thèmes de travail :

- la mise en œuvre de la loi de programmation militaire et de la loi relative au renseignement ;

- le renforcement des moyens de contrôle de la mise en œuvre des techniques de recueil du renseignement ;

- l'accroissement des moyens humains et techniques des services de renseignement ;

- l'évaluation de l'action des services de renseignement.

La délégation s'est plus particulièrement consacrée, cette année, à la préparation de l'examen parlementaire du projet de loi relatif au renseignement, prolongé par celui de la proposition de loi relative aux mesures de surveillance des communications électroniques. Elle a donné un avis sur l'économie générale du premier texte, sous la forme d'une lettre au Premier ministre⁽¹⁾. Quatre de ses membres ont été, dans leurs assemblées respectives, rapporteurs au fond ou pour avis de l'un ou l'autre de ces textes.

En début d'année (réunion du 19 février), elle a également entendu le rapport de la Commission de vérification des fonds spéciaux (CVFS) sur les comptes de l'exercice 2013.

Par ailleurs **la délégation a été consultée** par la mission de l'Inspection des services de renseignement sur l'élaboration du rapport d'activité des services de renseignement (*voir infra*)

Au titre de ses activités internationales, son président ou ses membres ont conduit des entretiens avec le Général Clapper, directeur du renseignement national (DNI) des États-Unis, le 28 janvier et les instances parlementaires assurant le contrôle de la politique publique du renseignement du Japon (5 octobre) et de Suisse (21 octobre).

Enfin, deux de ses membres ont participé à la **formation des stagiaires de l'Académie du renseignement**, au cours des sessions qui se sont tenues les 24 mars et 5 octobre.

⁽¹⁾ Cette lettre a été publiée dans un communiqué de presse de la délégation en date du 25 mars 2015.

Calendrier des réunions de la délégation parlementaire au renseignement en 2015

Réunion de travail du 14 janvier

Réunion du 22 janvier :

- Audition commune du Premier ministre, du ministre de la Défense et du ministre de l'Intérieur.

Réunion du 5 février :

- Audition du préfet Alain Zabulon, Coordonnateur national au renseignement ;
- Audition de M. Patrick Calvar, DGSI.

Réunion du 19 février :

- Présentation du rapport de la CVFS sur les comptes de l'exercice 2013.

Réunion du 24 mars :

- Examen du projet de loi relatif au renseignement, adopté par le Conseil des ministres le 19 mars.

Réunion du 28 mai :

- Audition de M. Patrick Calvar, DGSI ;
- Audition de M. Bernard Bajolet, DGSE.

Réunion de travail du 4 juin

Réunion du 22 juin :

- Audition de M. Didier Le Bret, CNR.

Réunion du 16 juillet :

- Audition du contre-amiral Bruno Durteste, directeur du GIC ;
- Audition de M. Jean-Marie Delarue, président de la CNCIS ;
- Audition de M. Cyrille Chabauty, conseiller technique « sécurité » au cabinet du Premier ministre.

Réunion du 3 septembre :

- Audition de M. Patrick Calvar, DGSI ;
- Audition de M. René Bailly, DRPP ;
- Audition du général de corps d'armée Michel Pattin, DOE, et du colonel Pierre Sauvegrain, SDAO, Direction générale de la Gendarmerie nationale ;
- Audition de Jérôme Léonnet, SCRT.

Déplacement au siège de la DGSE, le 15 octobre 2015 :

- Présentation par la direction technique des outils et de leur mise en œuvre ;
- Audition du directeur général, M. Bernard Bajolet.

Réunion du 5 novembre :

- Audition de M. Jean-Baptiste Carpentier, délégué interministériel à l'intelligence économique ;
- Audition de M. Francis Delon, président de la CNCTR.

Réunion du 26 novembre :

- Audition commune de MM. Patrick Calvar, DGSI, et Bernard Bajolet, DGSE.

Réunion du 17 décembre :

- Audition du général de corps d'armée Christophe Gomart, DRM.

II. LES INNOVATIONS INTRODUITES PAR LA LOI RELATIVE AU RENSEIGNEMENT

Le projet de loi relatif au renseignement a été annoncé par le Président de la République, à l'issue du deuxième Conseil national du renseignement, le 9 juillet 2014, et par le Premier ministre lors d'une intervention à l'UNESCO dans le cadre de l' *European Data Governance Forum*, le 8 décembre 2014. Il a été formellement présenté en Conseil des ministres, le 19 janvier dernier, au moment de l'annonce des mesures décidées à la suite des attentats survenus à Paris au début de l'année. Il ne s'agit pas d'un texte de circonstance car il procède d'une réflexion menée depuis plusieurs mois, s'appuyant notamment sur les travaux conduits par une mission

d'information de la commission des lois de l'Assemblée nationale⁽¹⁾ et sur ceux de la délégation parlementaire au renseignement.

Ce texte, devenu loi du 24 juillet 2015 relative au renseignement⁽²⁾, dote les activités de renseignement d'un cadre juridique, plus précisément décrit au chapitre II du présent rapport.

A titre subsidiaire, la loi du 24 juillet 2015 aménage le régime juridique applicable à la délégation parlementaire au renseignement fixé par l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires (*voir infra Chapitre IV*)

III. LE SUIVI DES PROPOSITIONS DE LA DÉLÉGATION

Année après année, la délégation parlementaire au renseignement formule, à l'occasion de son rapport annuel, des recommandations intéressant l'organisation et les moyens de services, comme le cadre juridique de leur action. L'an dernier, la délégation avait inséré pas moins de 104 propositions dans son rapport d'activité (*Voir annexe 2*)

Si certaines de ces préconisations ont pu être suivies d'effet, beaucoup sont demeurées lettre morte alors qu'elles conservent, aux yeux des membres de la délégation, toute leur actualité (*Voir annexe 3*)

Trois thèmes ont, plus particulièrement, motivé les recommandations de la délégation depuis 2012 : l'organisation du renseignement intérieur, la lutte contre la menace terroriste et le renseignement économique et financier.

A. LA LUTTE CONTRE LA MENACE TERRORISTE

Les attentats du vendredi 13 novembre 2015 sont encore dans tous les esprits. Leur simultanéité, le mode opératoire et le nombre de victimes leur confèrent une gravité sans précédent.

Cette attaque s'inscrit, dans une série d'attentats ou de tentatives d'attentats imputables à la mouvance djihadiste et remontant au mois de mars 2012, dont la délégation parlementaire au renseignement a eu, à chaque fois, à connaître :

- les 11 et 13 mars 2012, Mohammed Merah abat trois militaires à Toulouse et Montauban ; le 19, il tue trois enfants et un professeur à l'école juive d'Ozar Hatorah de Toulouse, avant d'être abattu le 22 mars ;

(1) Rapport d'information de MM. Jean-Jacques Urvoas et Patrick Verchère n° 1022 du 14 mai 2013 sur l'évaluation du cadre juridique applicable aux services de renseignement.

(2) Loi n° 2015-912 du 24 juillet 2015.

- le 7 janvier 2015, les frères Chérif et Saïd Kouachi tuent douze personnes au siège de Charlie Hebdo, dont les dessinateurs Wolinski, Cabu, Charb et Tignous, ainsi que deux policiers ; le surlendemain, retranchés dans une entreprise de Dammartin-en-Goële (Seine-et-Marne), les deux hommes sont abattus par les forces d'assaut ;

- le 8 janvier, Amédy Coulibaly tue une policière municipale, Clarissa Jean-Philippe, et blesse un agent municipal à Montrouge (Hauts-de-Seine) ; il prend plusieurs personnes en otage le lendemain dans une épicerie casher de la Porte de Vincennes, à Paris ; il tue quatre personnes avant d'être à son tour neutralisé ;

- le 3 février, Moussa Coulibaly blesse à l'arme blanche trois militaires en faction devant un centre de la communauté juive à Nice ;

- le 19 avril, Sid Ahmed Ghlam tente de voler la voiture d'Aurélie Châtelain et abat celle-ci ; il avouera aux enquêteurs avoir projeté un attentat, le lendemain, contre l'une des églises de Villejuif (Val de Marne) ;

- le 26 juin, Yassin Salhi tue son employeur sur le site de l'usine AirProducts, à Saint-Quentin-Fallavier (Isère) ; l'enquête révèle que le suspect est en lien avec la mouvance salafiste ;

- le 21 août, à bord du train Thalys reliant Amsterdam à Paris, Ayoub El Khazzani, armé d'un fusil d'assaut, blesse trois passagers avant d'être maîtrisé par des militaires américains en permission.

La permanence de la menace terroriste explique que la délégation ait, depuis trois ans, formulé chaque année des préconisations intéressant la lutte anti-terroriste.

En 2012, elle avait appelé à renforcer sensiblement les moyens de lutte contre le terrorisme (proposition n° 2) et, déjà, à doter notre pays des moyens permettant de suivre les déplacements de personnes par voie aérienne vers des destinations sensibles, y compris lorsque les trajets comportent une ou des escales (proposition n° 3). Le rapport pour l'année 2013 pointait une « *menace éman[ant] essentiellement de la mouvance islamiste radicale et djihadiste qui développe un discours très agressif à l'encontre de notre pays en raison de ses valeurs et de son engagement dans la lutte contre le terrorisme sur le territoire et sur la scène internationale* ».

L'an dernier, le rapport de la délégation était plus explicite encore puisqu'il appelait à mettre en place le système *Passenger Name Record (PNR)* à l'échelon national dans les plus brefs délais et promouvoir sa survenance à l'échelle européenne (proposition n° II-1), à mener une réflexion concernant l'amélioration du système européen de traitement des données d'enregistrement et de réservation – dit SETRADER – (proposition n° II-2) et à initier une amélioration du code frontières Schengen et notamment de son article 7 (proposition n° II-3).

La délégation prend acte de l'accord récemment trouvé au Parlement européen sur le PNR, dont la mise en place est soutenue de longue date par le gouvernement français. Elle restera attentive à une mise en application totale et rapide de ce dispositif (*voir infra p. 80*).

Elle prend également note de l'entrée en phase de production de SETRADER, avec un spectre limité à vingt compagnies aériennes pour des vols en partance ou en provenance de dix pays⁽¹⁾.

B. L'ORGANISATION DU RENSEIGNEMENT INTÉRIEUR

Faisant suite à une première réforme du renseignement intérieur effectuée en 2008, une nouvelle réorganisation est intervenue en mai 2014 afin de favoriser la complémentarité et la coopération des entités chargées de collecter les informations essentielles à la sécurité de nos concitoyens.

Ainsi, la Direction centrale du renseignement intérieur (DCRI) a-t-elle disparu au profit de la Direction générale de la sécurité intérieure (DGSI), tandis que la Sous-direction à l'information générale (SDIG) a laissé place au Service central de renseignement territorial (SCRT).

La délégation parlementaire au renseignement a accompagné ces transformations du renseignement intérieur. Dans son rapport pour 2012, elle préconisait déjà la transformation de la DCRI en direction générale, estimant indispensable que celle-ci dispose d'une autonomie de gestion notamment de son personnel. De même, elle a constamment et fortement souligné que l'articulation entre les services départementaux d'information générale et les services de la DCRI n'était pas suffisamment efficace.

Accueillant avec satisfaction la création de la DGSI, la délégation a veillé à ce que la nouvelle direction générale dispose des moyens nécessaires à cette autonomie. Son rapport de l'an dernier appelait ainsi à trouver très rapidement de nouvelles implantations immobilières pour accueillir les agents nouvellement recrutés (proposition n° VI-2). Le renouvellement, au début de cette année, de la prise à bail du site *** pour accueillir une partie des effectifs supplémentaires de la nouvelle direction générale constitue une première réponse aux inquiétudes de la délégation. Le site *** est en effet situé à proximité de celui de Levallois-Perret, siège de la DGSI.

La question du positionnement de la DRPP par rapport aux autres services de renseignement a également été évoquée, avec constance, par la délégation. Dans son dernier rapport, celle-ci constatait que cette direction de la préfecture de police agit en grande partie comme un service de renseignement sans bénéficier des moyens afférents. La délégation préconisait, par conséquent, « *une intégration dans la communauté du*

(1) Les pays concernés sont : l'Algérie, l'Égypte, le Liban, le Mali, le Maroc, la Mauritanie, le Niger, le Tchad, la Tunisie et la Turquie.

renseignement, même si elle consacrerait un discutable particularisme territorial ». Cette réflexion, qui concernait plus largement le statut du SCRT et de la SDAO, devait se traduire dans la loi relative au renseignement par la mise en place d'une communauté du renseignement dotée d'un premier et d'un second cercle - ce dernier se limitant, dans l'esprit du législateur, à ces quelques services.

D'autres recommandations ont été formulées ces trois dernières années, comme le souhait exprimé en 2014 de voir la DGSI rationaliser ses implantations territoriales (proposition n° VI-1), n'ont pas été, pour l'heure, suivies d'effet.

C. LA GESTION DES RESSOURCES HUMAINES

Dans son rapport pour 2012, déjà, la délégation recommandait de renforcer les moyens en personnel des services et de moderniser les conditions de gestion de ces ressources :

- proposition n° 7 : Poursuivre le renforcement des effectifs de la DGSE, de Tracfin et de la DNRED, ainsi que ceux de la DCRI (devenue DGSI).
- proposition n° 8 : Diversifier le recrutement de la DCRI en lui permettant notamment de recruter des contractuels, linguistes ou spécialistes de haut niveau, ce qui nécessite de lui accorder une véritable autonomie de gestion.
- proposition n° 9 : Poursuivre la modernisation de la gestion des ressources humaines, la diversification du recrutement et l'amélioration de la mobilité entre les services.

Depuis deux ans, dans un contexte marqué par la menace terroriste, la délégation a pris acte des annonces successives de recrutements tout en mettant en garde contre la tentation de redéployer au profit exclusif de la lutte anti-terroriste des effectifs dédiés à d'autres missions essentielles, par exemple le contre-espionnage et à la sécurité économique à la DGSI (proposition n° VI-3 du rapport 2014).

Parallèlement à la réorganisation du renseignement intérieur intervenue en 2013-2014, la priorité donnée à la lutte contre le terrorisme s'est traduite par l'annonce de la création de 432 postes à la DGSI et de 203 postes au SCRT, dans le cadre d'un plan quinquennal 2013-2018. A la suite des attentats de janvier 2015, il a été annoncé dans le cadre des plans consécutifs aux attentats de janvier (plan de lutte anti-terroriste - PLAT-) et novembre 2015 (pacte de sécurité) que *** à *** emplois nouveaux seront alloués d'ici 2017 aux services concourant au renseignement intérieur¹. La

¹ Le CNR n'a pas été en mesure de communiquer à la délégation un prévisionnel précis des plafonds d'emplois pour 2016, les arbitrages de programmation budgétaire initiale n'ayant pas encore été

DGSI bénéficie dans le cadre du PLAT de 500 emplois de 2015 à 2017 et dans le cadre du plan de sécurité de *** emplois de 2016 à 2017.

Désormais rattachée directement au ministre de l'Intérieur conformément au décret n° 2014-445 du 30 avril 2014, la DGSI constitue le principal service de renseignement intérieur, chargé à la fois :

- du contre-espionnage,
- de la contre-ingérence économique et de la contre-prolifération,
- de la lutte contre le terrorisme et les extrémismes violents,
- de la lutte contre la grande criminalité organisée et la cyber-criminalité.

En début d'année 2015, la DGSI comptait 3 300 agents. Elle bénéficiera donc de *** postes supplémentaires jusqu'en 2017 (tous plans confondus) et, en 2018, du reliquat de *** emplois au titre du Plan quinquennal.

A Paris et dans la région parisienne, la DGSI est renforcée par la DRPP, en application du décret du 30 avril 2014 précité qui précise que « *le service chargé, sous l'autorité du Préfet de police, des 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* ». Cette dernière dispose d'effectifs plus restreints, soit 850 fonctionnaires de police. Dans le cadre du PLAT, la DRPP pourra créer 100 postes supplémentaires, dont *** affectés aux missions de renseignement, selon les informations transmises par le Coordonnateur national du renseignement (voir Annexe 4).

Le SCRT a ainsi bénéficié d'un important renforcement de ses effectifs en charge de la lutte contre la radicalisation. Alors que le service ne comportait que 1 507 postes à sa création au 1^{er} septembre 2014, il compte désormais 2 000 fonctionnaires. Ses moyens seront accrus de *** postes de personnels actifs d'ici 2018, dont 150 postes ont déjà été pourvus sur l'année 2015¹. Par ailleurs, *** recrutements d'agents contractuels dans diverses spécialités (expert en informatique, psychologue, interprète...) sont prévus sur la même période et *** adjoints administratifs ont été affectés au service au troisième trimestre 2015.

De son côté, la SDAO ne totalisait que 39 personnels lorsqu'elle a été créée au 1^{er} janvier 2014. Elle compte désormais 67 personnels : *** militaires et *** personnels civils, auxquels s'ajoutent *** fonctionnaires de la police nationale détachés du SCRT. Ces moyens ont été dégagés, au moment de sa création, par redéploiements internes à la Gendarmerie nationale. En 2015, *** créations de postes ont toutefois bénéficié à la sous-direction dont *** ont été financées par le PLAT. Si ces effectifs peuvent paraître modestes, la

rendus après l'annonce du recrutement de 5 000 policiers et gendarmes ainsi que de 1 000 douaniers, dans le cadre du pacte de sécurité.

¹ Selon les informations recueillies par la délégation, ces 150 recrutements se répartissaient ainsi.***

délégation rappelle que la SDAO s'appuie sur les bureaux renseignement des régions ainsi que les cellules et officiers adjoints renseignement des groupements de gendarmerie, soit *** militaires.

La direction nationale du renseignement et des enquêtes douanières (DNRED), au sein de la direction générale des douanes, employait, en 2014, 712 agents. Dans le cadre du PLAT, et du plan de lutte contre le financement du terrorisme présenté le 24 novembre dernier, le Gouvernement a annoncé la création de 70 nouveaux postes au sein de la DGDDI, dont *** à la DNRED. La délégation note que la DNRED a créé à l'automne 2015 un réseau de correspondants « terrorisme » dans ses services locaux. Ces derniers auront pour mission d'échanger, sur le terrain, avec les services spécialisés de la DGSI et du SCRT et de faire office d'interface avec l'ensemble des services locaux des douanes.

Enfin, la délégation relève que depuis deux ans le plafond des emplois accordés à TRACFIN a été sensiblement revalorisé, passant de 94 en 2013 à 118 en 2015. 6 emplois ont été créés, cette année, dans le cadre du PLAT. Toutefois, la création de 50 ETPT supplémentaires recommandée dans le rapport pour 2014 (proposition n° III-4) ne sera pas atteinte à court terme.

Par ailleurs, afin de stabiliser ses effectifs, la DPSD s'était vu attribuer, au titre de la LPM initiale un effectif terminal de 1 100 personnes au 31 décembre 2015. À cette fin, un droit complémentaire à recrutement de *** postes avait été octroyé au service pour 2015. En raison du contexte, des droits à recruter supplémentaires ont été alloués au service, en premier lieu au titre du plan gouvernemental de lutte anti-terroriste annoncé par le Premier ministre à la suite des attentats du 11 janvier 2015 (***, soit *** en 2015 et *** en 2016) et en second lieu, au titre de l'actualisation de la LPM (*** de 2016 à 2018).

Les autres services relevant du ministère de la défense ont connu des renforcements significatifs soit au titre de la loi du 18 décembre 2013 de programmation militaire pour 2014-2019 et de la loi d'actualisation du 28 juillet 2015 (DGSE et DRM) certaines (DGSE) comprenant les mesures annoncées par le Premier ministre le 21 janvier 2015 dans le cadre de la lutte contre le terrorisme (*voir infra p. 49 et 52*).

D. LE RENSEIGNEMENT ÉCONOMIQUE ET FINANCIER

L'an dernier, la délégation avait retenu le renseignement économique et financier (REF), comme premier axe de travail, pointant « *sa trop faible prise en compte dans la politique publique du renseignement* ».

Après avoir constaté la permanence d'un espionnage économique agressif, le rapport 2014 formulait vingt-deux propositions relatives au REF, dont trois concernaient spécifiquement le dispositif public d'intelligence économique :

- proposition n° III-19 : Maintenir le service de coordination de l'intelligence économique (SCIE) auprès du secrétaire général des ministères de l'économie et des finances ;
- proposition n° III-20 : Nommer le chef du SCIE adjoint du délégué interministériel à l'intelligence économique (D2IE) ;
- proposition n° III-22 : Maintenir les efforts accomplis en faveur d'un dispositif public d'intelligence économique efficace, coordonné et en prise avec le REF.

En cette matière, le D2IE joue un rôle central : il élabore et propose la politique publique d'intelligence économique ; il en anime et coordonne également la mise en œuvre. Directement rattaché au Premier ministre depuis 2013, il s'appuie sur une structure légère, reposant sur un réseau de correspondants dans les ministères et les préfetures, ainsi que dans les collectivités territoriales qui souhaitent s'y associer.

Afin d'exercer un droit de suite, la délégation a procédé, au cours de sa réunion du 5 novembre 2015, à l'audition de M. Jean-Baptiste Carpentier, nommé D2IE à compter du 3 août 2015 et, par ailleurs, ancien directeur de TRACFIN de 2008 à 2015. Le nouveau délégué a expliqué que, conformément au souhait exprimé par le Premier ministre⁽¹⁾, le dispositif français d'intelligence économique sera réformé afin de rassembler au sein d'une entité unique associée aux administrations financières l'ensemble des moyens auparavant répartis entre la D2IE et le SCIE. Cette nouvelle entité sera notamment chargée de veiller à la sécurité économique de la Nation, au sens de l'article L. 1142-3 du code de la défense ; elle doit permettre aux services de la communauté du renseignement de travailler plus efficacement avec les administrations financières.

Dans sa réponse au questionnaire adressé par la délégation, le ministre des Finances et des comptes publics indique qu' « *il sera ainsi créé en 2016, auprès du ministre de l'économie, une fonction de commissaire à l'information stratégique et à la sécurité économique, disposant d'un service à compétence nationale dédié, placé au sein de la direction générale des entreprises.* » (Voir Annexe 3).

La délégation avait pourtant salué, dans son rapport 2014, le rattachement de la D2IE auprès du Premier ministre comme un moyen utile de consacrer la dimension interministérielle de son action. Elle regarde donc avec circonspection ce changement de tutelle et sera attentive à la traduction concrète, au cours des prochains mois, des orientations qui lui ont été présentées.

¹ Lettre de mission du Premier ministre en date du 13 juillet 2015.

CHAPITRE II - LA MISE EN ŒUVRE PROGRESSIVE DE LA LOI SUR LE RENSEIGNEMENT

I. UNE LOI LARGEMENT INSPIRÉE DES TRAVAUX DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

A. LA REPRISE PAR LA LOI DU 24 JUILLET 2015 DE L'ESSENTIEL DES PRÉCONISATIONS FORMULÉES EN 2014

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement s'est inspirée de plusieurs travaux, en particulier du rapport de la délégation pour l'année 2014¹. Un grand nombre des propositions de la délégation ont inspiré le projet de loi initial ; d'autres ont été insérées au cours des débats au Parlement.

1. Le choix d'un cadre d'action des agents, pour des finalités précisées

Le choix d'un cadre d'activité a été justifié par les trois avancées essentielles qu'il permet : **consacrer les libertés individuelles, légitimer l'action des services et protéger les agents des services spécialisés**, pour lesquels cette dernière avancée était particulièrement nécessaire.

La loi relative au renseignement précitée a ainsi prévu la possibilité de mettre en œuvre des techniques de renseignement au titre de plusieurs finalités, précisées à l'article L. 811-3 du code de la sécurité intérieure².

Les finalités des actions pouvant justifier l'autorisation et la mise en œuvre sur le territoire national des techniques de renseignement (art. L. 811-3)

- 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale
- 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
- 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
- 4° La prévention du terrorisme ;
- 5° La prévention :
 - a) des atteintes à la forme républicaine des institutions ;

¹ Délégation parlementaire au renseignement, Rapport d'activité 2014, contrôler les services de renseignement - An I, n° 2482 (Assemblée nationale) et 201 (Sénat) et du rapport d'information de MM. Urvoas et Verchère précité.

² En conformité avec la proposition n° 4 du chapitre IV du rapport précité.

- b) des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;
- c) des violences collectives de nature à porter gravement atteinte à la paix publique ;
- 6° La prévention de la criminalité et de la délinquance organisées ;
- 7° La prévention de la prolifération des armes de destruction massive.

L'article L. 811-2 du code de la sécurité intérieure précise quant à lui le cadre général d'action des agents en France et à l'étranger.

A l'étranger, outre qu'un chapitre précise le cadre d'action applicable - la proposition de loi relative à la surveillance internationale a permis d'adopter ces dispositions initialement introduites par la loi du 24 juillet 2015 mais censurées par le Conseil constitutionnel¹ pour incompétence négative - les agents agissant à l'étranger sont désormais protégés, en application notamment de l'article L. 862-1 du code de la sécurité intérieure, qui impose au procureur de la République territorialement compétent ayant connaissance de faits commis hors du territoire national, par un agent des services pouvant constituer des infractions pénales, d'en informer préalablement le ministre dont l'agent relève avant tout acte de poursuite.

Par ailleurs, l'**anonymat des agents** a été également conforté en dispensant de publication les délégations de signature accordées.

2. Le renforcement des garanties des citoyens

La délégation avait souligné la nécessité de **renforcer les garanties des citoyens**, en particulier, en imposant que le recueil des données de connexion, prévu par l'article L. 246-1 du code de la sécurité intérieure s'effectue dans le respect de l'article 226-15 du code pénal qui protège le secret des correspondances².

La loi relative au renseignement du 24 juillet 2015 a pris en compte cette proposition, en l'étendant à **l'ensemble des techniques de renseignement** mises en œuvre par le chapitre 1^{er} du livre VIII, relatif au recueil des données techniques de connexion.

Cette extension se justifie par le fait que toutes ces techniques mobilisent des données de connexion. La protection de l'article 226-15 permet donc de garantir que la collecte des données de connexion ne doit pas permettre d'accéder aux contenus.

¹ Décision n° 2015-713 DC du 23 juillet 2015 : <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html>

² Proposition n° 14 du chapitre IV.

La mise en place d'une procédure de contrôle de légalité et de proportionnalité de l'action des services par la nouvelle autorité administrative indépendante¹ s'est quant à elle effectuée selon des modalités dans l'esprit des orientations proposées par la délégation. En effet, en application de l'article L. 841-1 du même code, toute personne souhaitant vérifier qu'aucune technique n'a été mise en œuvre à son égard peut, après avoir saisi la CNCTR d'une demande en ce sens², saisir le Conseil d'État. Enfin, le président ou au moins trois membres de la commission peuvent également le saisir, si leur avis n'a pas été suivi par le Premier ministre.

3. L'attribution de techniques nouvelles, pour certaines inspirées des techniques applicables en police judiciaire

La délégation avait également préconisé de **transposer en police administrative un certain nombre de techniques spéciales de police judiciaire**³. Cette proposition a été également largement suivie.

En effet, la loi relative au renseignement transpose et modernise en police administrative les techniques utilisables en police judiciaire dans le cadre de **la lutte contre la criminalité organisée**, comme la possibilité de sonoriser un lieu privé, la captation de données informatiques ou l'intrusion domiciliaire.

En effet, jusqu'à la loi du 24 juillet 2015, les services de renseignement ne disposaient que des **interceptions de sécurité**, du **recueil des données de connexion** et, depuis le 1^{er} janvier 2015, de la possibilité de **géolocaliser un terminal « sur sollicitation du réseau et transmis en temps réel par les opérateurs**⁴ ».

Certaines techniques désormais autorisées dans le cadre de la police administrative n'existent pas en police judiciaire, en raison de leur objectif purement préventif, comme le dispositif technique de l'article L. 851-2, permettant de recueillir en temps réel sur les réseaux des documents ou des données relatives à des personnes préalablement identifiées comme présentant une menace, ou la possibilité d'imposer la mise en place sur les réseaux d'un dispositif technique permettant de détecter des connexions susceptibles de révéler une menace terroriste (L. 851-3).

¹ Propositions n° 21 et 22 du chapitre IV.

² La saisine de la CNCTR est un recours administratif préalable obligatoire.

³ Proposition n° 16 du chapitre IV.

⁴ Article L. 246-3 du code de la sécurité intérieure

4. Le maintien de la centralisation des éléments collectés

La **centralisation des données collectées**, qui est le choix qui a été historiquement fait dans le cadre du contrôle exercé par la CNCIS, est un élément déterminant du contrôle.

Cette centralisation est assurée par un service rattaché au Premier ministre, le **Groupement interministériel de contrôle** (GIC).

Toutefois, si cette fonction était assurée pour les quelques techniques de renseignement permises par la loi du 10 juillet 1991, les nouvelles techniques de renseignement autorisées, en particulier les instruments portables, *******, posent une difficulté.

Le rôle du GIC est donc essentiel pour définir un système permettant à la CNCTR d'accéder d'une manière simple à l'ensemble des données collectées.

*******la centralisation des données est un élément stratégique, en permettant d'éviter les doublons mais en permettant surtout de rendre le contrôle de la CNCTR **effectif**.

5. Le choix d'une structure aux moyens et aux pouvoirs adaptés aux nouveaux enjeux du contrôle

Dans son rapport pour l'année 2014, la délégation avait préconisé la création d'une autorité administrative indépendante (AAI) remplaçant la CNCIS, en la dotant de moyens « *considérablement accrus* »¹, en accroissant le nombre de ses membres² et en supprimant les parlementaires membres³ ainsi que la personnalité qualifiée instituée par l'article 20 de la loi de programmation militaire du 18 décembre 2013⁴.

Si la majeure partie de ces propositions a été prise en compte par la loi sur le renseignement, les parlementaires ont été maintenus dans la nouvelle AAI créée, leur nombre étant même porté de deux à quatre.

Toutefois, le collège a été complété par une **personnalité qualifiée** nommée sur proposition de l'Autorité de régulation des communications électroniques et des postes (ARCEP).

En effet, certaines techniques de renseignement nouvelles nécessiteront de la part de la CNCTR une **expertise technique approfondie** pour exercer un contrôle effectif, en particulier sur le dispositif de suivi en temps réel de personnes préalablement identifiées comme présentant une menace terroriste (article L. 851-2) ou le dispositif technique permettant de

¹ Proposition n° 9.

² Proposition n° 10.

³ Proposition n° 11.

⁴ Proposition n° 15.

détecter des connexions susceptibles de révéler une menace terroriste (article L. 851-3).

6. L'extension des pouvoirs de contrôle de la DPR

Conséquence du renforcement des pouvoirs des services de renseignement, les prérogatives de contrôle de la délégation ont été accrues (*voir infra p. 89 et suiv.*).

B. LE CHOIX CONTESTABLE DE NE PAS AVOIR PARACHEVÉ LE SYSTÈME PAR UN RENFORCEMENT SUBSTANTIEL DE L'INSPECTION DES SERVICES DE RENSEIGNEMENT

Certaines propositions de la délégation n'ont été que partiellement retenues.

Le renforcement de **l'inspection des services de renseignement**¹, dont il a été indiqué que la pérennisation était à l'étude, s'avèrerait pourtant nécessaire, tout comme la désignation d'un chef d'inspection qui avait été recommandée l'an dernier. Il est, à cet égard, précieux pour la délégation de prendre connaissance de ses analyses, comme elle a pu le faire avec les rapports *** qui lui ont été transmis au mois d'octobre 2015.

C. LE REFUS D'UNE EXTENSION DES POUVOIRS DE LA CNCTR EN MATIÈRE DE CONTRÔLE DES FICHIERS

Dans le rapport précité pour l'année 2014, la délégation avait suggéré plusieurs modifications de la loi informatique et liberté, en **transférant à la nouvelle AAI des prérogatives ou des possibilités de contrôle de l'utilisation des fichiers**.

En effet, plusieurs propositions avaient pour objet de permettre une exploitation plus large des fichiers par les services de renseignement, en permettant en particulier leur **interconnexion**².

Toutefois, le refus du Gouvernement de le permettre a rendu partiellement caduques deux autres propositions, qui étaient la conséquence de cette possibilité nouvelle, visant à confier le contrôle des fichiers de services de renseignement à l'AAI chargé du contrôle de la mise en œuvre des techniques de renseignement³ et à confier à **l'inspection des services de renseignement** une mission de contrôle des fichiers de souveraineté⁴.

¹ Proposition n° 6.

² Proposition n° 17.

³ Proposition n° 18.

⁴ Proposition n° 19.

Il a été toutefois décidé de confier une mission de contrôle des fichiers de souveraineté à l'inspection des services de renseignement à l'issue de laquelle il sera décidé, le cas échéant, de donner une forme de périodicité.

II. UNE MONTÉE EN PUISSANCE PROGRESSIVE DES ACTEURS DU CONTRÔLE

A. LA MISE EN PLACE DE LA CNCTR, EN PHASE DE MONTÉE EN PUISSANCE

1. Le maintien et le renforcement des moyens de contrôle de la CNCIS

L'effectivité du contrôle exercé par la CNCIS sur les interceptions de sécurité était principalement liée à la **centralisation des éléments collectés**. En particulier, la possibilité de consulter aussi bien les données relatives aux autorisations que les retranscriptions écrites des conversations comme des conversations elles-mêmes avaient été identifiées par la commission des lois du Sénat comme un élément déterminant du contrôle, conditionnant en réalité l'effectivité de celui-ci¹.

Les dispositions applicables à la CNCIS ont été maintenues au bénéfice de la CNCTR, qui dispose d'un accès aux données relatives aux interceptions de sécurité dans les mêmes conditions que pour la CNCIS. La CNCTR note une nette augmentation du nombre de demandes d'interceptions de sécurité qui lui sont soumises par rapport à celles présentées à la CNCIS.

En effet, à l'initiative de M. Philippe Bas, président de la commission des lois du Sénat et membre à ce titre de la délégation, rapporteur de la loi relative au renseignement, un amendement a été adopté par la commission des lois pour préciser que « *la CNCTR dispose d'un accès direct, immédiat et permanent aux données recueillies, aux transcriptions et aux extractions effectuées par le GIC* ». M. Philippe Bas a par ailleurs souhaité insister sur le fait que « *l'ensemble de ce qui a été collecté, sans aucun tri préalable par les services ni choix par eux des éléments à transmettre, doit être mis à la disposition de la CNCTR, qui disposera ensuite de la possibilité d'y accéder en permanence* ».

Pour les nouvelles techniques de renseignement, cette obligation de centralisation est également applicable. Toutefois, la CNCTR a exigé de pouvoir disposer d'un accès permanent, complet et direct aux données issues de toutes les techniques de renseignement. Elle s'appuie sur le GIC qui centralise toutes les données issues des interceptions de sécurité et de

¹ Rapport n° 460 (2014-2015), sur le projet de loi relatif au renseignement et sur la proposition de loi organique présentée par MM. Jean-Pierre Raffarin et Philippe Bas, relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement, p.79.

géolocalisation en temps réel. Elle entend s'appuyer également sur lui pour les nouvelles techniques.

***.

2. Une montée en puissance progressive des moyens de la CNCTR

La Commission nationale du contrôle des techniques de renseignement a été installée **le 3 octobre 2015**, dans les locaux de l'ancienne CNCIS.

Opérer un bilan de son activité seulement trois mois après son installation est encore prématuré, d'autant que certaines mesures d'application de la loi sur le renseignement sont encore en cours d'élaboration ou viennent tout juste d'être adoptées. Ainsi, le décret relatif aux services du « deuxième cercle » a été pris seulement le 12 décembre dernier et la personnalité qualifiée auprès du Premier ministre¹ est restée en activité, en attente du décret transférant sa compétence à la CNCTR. Ce décret du Premier ministre, dit « données de connexions », a été effectivement publié le 31 janvier 2016².

Toutefois, plusieurs enseignements peuvent être retenus sur cette courte période. En effet, à la mi-janvier 2015, la CNCTR a rendu plus de *** avis sur des demandes de mise en œuvre de technique de renseignement. Plus de *** étaient relatives aux interceptions de sécurité. Près de *** portaient sur des demandes de géolocalisation en temps réel et plus de *** sur des nouvelles techniques de renseignement.

Sur les *** demandes concernant les nouvelles techniques de renseignement, une proportion significative concerne *** et dans une moindre mesure, les autres techniques de renseignement, ***.

Au regard de l'augmentation prévisionnelle de l'activité de la CNCTR, par rapport à l'activité de la CNCIS, les effectifs de la nouvelle AAI ont été portés de 7 agents, que comptait l'ancienne CNCIS, à **10 ETPT d'ici la fin de 2015** et devrait compter **18 agents d'ici la fin de l'année 2016**. La CNCTR a recruté, au 1^{er} janvier 2016, un secrétaire général, ainsi que des personnels experts.

Lors de son audition par la délégation, le président de la CNCTR, M. Francis Delon, a estimé que ces augmentations d'effectifs étaient suffisantes pour permettre à la CNCTR de remplir ses objectifs.

Il a également souligné que la CNCTR dispose, outre de la personnalité qualifiée nommée par l'ARCEP, d'un ingénieur *** et

¹ Cette personnalité qualifiée, placée auprès du Premier ministre autorise l'accès administratif aux données de connexion. ***

² Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

désormais, de ce fait, des compétences techniques nécessaires pour exercer effectivement son contrôle.

Les crédits de fonctionnement et d'investissement bénéficieraient d'une augmentation très substantielle par rapport aux crédits dont la CNCIS disposait, puisqu'ils seraient multipliés par cinq, afin d'être portés de **580 000 euros (AE-CP) pour 2015 à 2,2 millions d'euros (AE-CP) pour l'année 2016**. Par un amendement adopté au cours des débats à l'Assemblée nationale, le budget de l'AAI a même été finalement porté à **2,9 millions d'euros (AE-CP)¹**.

L'accès administratif aux données de connexion s'effectue encore après l'autorisation d'une personnalité qualifiée placée auprès du Premier ministre depuis la loi n° 2013-1168 du 18 décembre 2013 relative à la lutte contre le terrorisme qui reçoit directement des services les demandes d'autorisation.

Après la publication du décret transférant cette compétence à la CNCTR, ces demandes se feront par le biais de la CNCTR, selon une procédure semblable à celle existant actuellement : les services saisiront directement la CNCTR de leurs demandes et le GIC assurera l'interface avec les opérateurs. Ce décret a été publié le 31 janvier 2016.

3. Le constat d'importantes différences par rapport à la CNCIS

a) La collégialité

Le caractère **collégial** de la CNCTR est un élément nouveau par rapport à la CNCIS, dont la composition était limitée à un président et à deux parlementaires.

Au-delà d'un nombre de membres porté à neuf, la loi consacre elle-même cette collégialité, en imposant que certaines décisions soient prises en formation plénière ou restreinte, en cas d'intrusion domiciliaire ou en cas de mesures prises à l'encontre d'une profession protégée.

D'une manière générale, l'article L. 832-3 prévoit même que toute question nouvelle ou sérieuse doit être tranchée par la formation plénière ou restreinte de la Commission. Ainsi, la définition de la notion de « professions protégées » a été arrêtée en formation plénière par la CNCTR.

Depuis sa création, la CNCTR se réunit de façon régulière trois fois par semaine en formation restreinte et une fois toutes les trois semaines en formation plénière. Par ailleurs, les formations plénières et restreintes

¹ Un amendement n° II-239 accorde 750 000 euros supplémentaires à la CNCTR, mais un amendement n° II-10 diminue de 718 000 euros les crédits du programme « protection des droits et des libertés ». Toutefois, au regard de la motivation de ce dernier amendement, cette diminution ne semble pas concerner la CNCTR mais d'autres AAI (en particulier la CNIL et le Défenseur des droits).

peuvent être convoquées en urgence pour examiner, conformément à la loi, dans les 72 heures, les demandes impliquant une introduction dans un domicile ou celles portant sur une personne, de nationalité française ou étrangère, exerçant une profession protégée. Cette situation nouvelle entraîne **d'importantes contraintes** pour ses membres, en particulier les parlementaires, que la délégation avait recommandé d'exclure pour les remplacer par des personnalités qualifiées.

Par ailleurs, le président de la CNCTR a fait le choix que la formation plénière comporte, en principe, toujours **au moins un parlementaire**, alors même que les règles de *quorum* pourraient permettre à la CNCTR de statuer sans parlementaire.

Le recours juridictionnel n'a toutefois pas encore été expérimenté, qu'il concerne le particulier demandant qu'il soit vérifié qu'il ne fait pas l'objet de mesures de surveillance indues ou qu'il ait été initié par la CNCTR, en cas de refus du Premier ministre de suivre son avis. **À ce jour, tous les avis de la CNCTR ont été suivis par le Premier ministre.**

b) La pression inédite d'un contrôle juridictionnel

L'instauration d'un recours juridictionnel effectif du Conseil d'État au bénéfice de la CNCTR ainsi que la possibilité pour toute personne s'estimant l'objet d'une mesure de surveillance de former un recours devant le Conseil d'État crée une pression sur la qualité des procédures suivies, aussi bien par les services que par la CNCTR.

En effet, les membres du Conseil d'État appartenant à la formation spécialisée auront accès à l'ensemble des documents relatifs à l'autorisation en cas de contentieux. Cette situation nécessite en particulier de disposer d'une compétence juridique au sein des services pour apprécier la faisabilité d'une demande exprimée par un opérateur.

La mise en œuvre effective de recours juridictionnels devrait permettre de renforcer encore l'effectivité de ce contrôle.

B. LE SOUS-DIMENSIONNEMENT DU GROUPEMENT INTER-MINISTÉRIEL DE CONTRÔLE (GIC) POUR RÉPONDRE AUX DÉFIS POSÉS PAR LA LOI DU 24 JUILLET 2015

1. Le positionnement ambigu du GIC, à l'organisation perfectible

Le **Groupelement interministériel de contrôle** (GIC) est, avec la CNCTR, une structure qui sera particulièrement mobilisée dans les semaines à venir mais il sera aussi un **acteur clef du contrôle**, en étant l'intermédiaire technique entre la CNCTR et les services.

Le GIC a fonctionné avec 127 personnes en 2014, - soit 75 ETPT mis à disposition par le ministère de la défense et 52 contractuels recrutés directement par le GIC***.

Pour la mise en œuvre de la loi relative au renseignement, les effectifs du GIC devraient passer progressivement à *** au 31 décembre 2015, *** au 31 décembre 2016 pour atteindre *** au 31 décembre 2020.

La place du GIC dans l'architecture générale mise en place par la loi et sa participation à la fonction de contrôle des services exigeait une clarification du statut de ses personnels.

S'agissant des contractuels, à compter de 2016, *** des crédits sont inscrits au programme 129 « coordination du travail gouvernemental », et un plafond d'emplois (80 ETPT) figure dans le programme annuel de performance annexé au projet de loi de finances.

S'agissant des emplois mis à disposition par le ministère de la défense, ils devraient être affectés au GIC avant le 1^{er} janvier 2017. Un droit d'option sera ouvert aux personnels concernés. ***. Les programmations des effectifs et des budgets devront être ajustées en conséquence. En effet, comme l'a souligné l'amiral Bruno Durteste lors de son audition par la délégation, le GIC est entré dans une phase évolutive, en particulier pour développer des systèmes d'information nécessaires pour assurer le respect de la loi relative au renseignement en assurant la traçabilité et le recueil des données en particulier pour les nouvelles techniques. Dès lors, il sera désormais envisageable de faire carrière au GIC.

Les personnels du GIC relèveront donc soit de la DSAF, soit du Secrétariat général de la défense et de la sécurité nationale (SGDSN) ***.

Il serait également hautement souhaitable que le GIC soit juridiquement consolidé en lui reconnaissant, à l'instar de l'ANSSI rattachée également au SGDSN, le statut de service à compétence nationale.

La DPR recommande l'affectation au GIC des personnels mis à disposition par le ministère de la défense avant le 31 décembre 2017 (Proposition n°1).

Elle propose l'attribution au GIC du statut de service à compétence nationale (Proposition n°2).

2. Le développement attendu d'une application informatique permettant de centraliser effectivement les demandes

Le schéma décisionnel entre la demande de la mise en œuvre d'une technique de renseignement et son autorisation par le Premier ministre, après avis de la CNCTR n'est pas modifié.

En effet, le GIC assure toujours un rôle de **centralisation** des demandes émanant des cabinets des ministres, qui centralisent eux-mêmes

les demandes des cabinets des directions générales demanderesse. Le GIC transmet ensuite les demandes pour avis à la CNCTR, puis après que celle-ci a rendu son avis, le GIC met alors la demande à la signature du Premier ministre – ou de l'un de ses délégués -, avant de retourner la demande au ministère concerné.

***, la mise en place d'un système informatique permettant de traiter rapidement les demandes par le GIC est nécessaire, au regard du nombre et de la diversité des techniques de renseignement désormais autorisées.

*** estime que l'application développée par le GIC *** répondra aux besoins attendus.

Toutefois, pour les nouvelles techniques utilisées de manière très décentralisées, ***, le programme informatique ne serait disponible que sous *** mois ***.

Au regard des enjeux du contrôle et du nombre de demandes attendues, ce développement doit être très rapidement mené : l'arbitrage technique sur ce sujet doit donc être rapidement rendu.

La DPR recommande que l'arbitrage technique * soit rendu par le Premier ministre dans les meilleurs délais (*Proposition n°3*).**

C. UNE DEMANDE DE MISE EN ŒUVRE DE NOUVELLES TECHNIQUES ENCORE RELATIVEMENT FAIBLE

Contrairement aux attentes, les demandes des services n'ont pas fortement augmenté, pour plusieurs raisons, aussi bien **conjoncturelles**, en raison de la publication tardive de certains décrets, en particulier le décret relatif aux services du second cercle, que **structurelles**, en raison des **difficultés techniques d'élaboration** de certaines techniques nouvelles.

1. Une augmentation des demandes difficile à évaluer préalablement

L'évaluation de l'augmentation des demandes adressées et de leur traitement par la CNCTR est relativement compliquée à mener.

*** évalue à *** l'augmentation des demandes pour l'année 2016, mais l'évaluation est relativement fragile.

Cette augmentation représenterait ainsi *** demandes au titre des **interceptions de sécurité**, *** demandes de mise en œuvre de nouvelles techniques de renseignement, ***, *** à *** demandes d'accès administratif aux données de connexion et *** demandes simples d'identifications.

2. La prudence de la DGSJ dans la mise en œuvre des techniques nouvelles ?

Lors de son audition, M. Francis Delon a également souligné que la DGSJ, qui est le principal service pouvant demander la mise en œuvre des nouvelles techniques de renseignement sur le sol national, a préféré adopter une attitude prudente, consistant à former préalablement les agents, en mettant en place un programme de formation ***.

Certains dispositifs nécessitent d'importants développements techniques préalables avant de pouvoir être mis en œuvre.

La DPR demande que les techniques de renseignement * puissent être mises en œuvre sans retard eu égard *** au niveau de la menace terroriste (*Proposition n°4*).**

D. LA PUBLICATION DES DÉCRETS D'APPLICATION

Si certains décrets d'application de la loi relative au renseignement ont été édictés dès la fin du mois de septembre 2015, soit seulement deux mois après la promulgation de la loi, d'autres ont été publiés en décembre 2015 et fin janvier 2016.

Ainsi le décret relatif à **l'accès administratif aux données de connexion** a-t-il été publié le 31 janvier 2016. Dans l'attente de la publication de ce décret, c'est le précédent dispositif élaboré en 2014 qui a continué à s'appliquer.

La DPR prend acte de la publication dans les délais requis des décrets d'application de la loi relative au renseignement.

III. LE DÉFI D'UN CONTRÔLE EFFECTIF DE LA MISE EN ŒUVRE DES NOUVELLES TECHNIQUES DE RENSEIGNEMENT

A. LES DIFFICULTÉS D'ÉTENDRE LE SCHÉMA APPLICABLE AUX TECHNIQUES PERMISES PAR LA LOI DU 20 JUILLET 1991 À CERTAINES TECHNIQUES NOUVELLES DE RENSEIGNEMENT

La procédure applicable avant la loi du 24 juillet 2015 concernant les techniques de renseignement permises antérieurement perdure. Le niveau de contrôle mené par la CNCTR sur ces techniques peut donc être considéré comme s'inscrivant dans les mêmes standards.

Il aurait été en effet paradoxal que la loi du 24 juillet 2015 diminue les garanties apportées en la matière.

Le morcellement de la mise en œuvre des techniques pose également la question de la centralisation des données collectées. ***

Il faut rappeler que le législateur a clairement posé comme principe que la CNCTR devait avoir **un accès permanent complet et direct aux données collectées, quel que soit finalement le choix du stockage retenu.** ***

La DPR demande que la CNCTR puisse avoir un accès permanent, complet et direct aux éléments collectés par les nouvelles techniques dans les conditions posées par la loi et dans des délais raisonnables (Proposition n°5).

B. UNE DÉSIGNATION TRÈS LARGE DES SERVICES POUVANT BÉNÉFICIER DE TECHNIQUES DU RENSEIGNEMENT COMPLIQUANT LE CONTRÔLE DE LA MISE EN ŒUVRE DES TECHNIQUES DE RENSEIGNEMENT

1. Une désignation extensive des services autorisés à recourir aux techniques de renseignement

En application de l'article L. 811-4 du code de la sécurité intérieure, **le décret du 11 décembre 2015¹** a désigné les services pouvant bénéficier de certaines techniques de renseignement, au titre de certaines finalités.

La délégation parlementaire au renseignement considère que l'extension des techniques de renseignement aux services de renseignement du « deuxième cercle » devait être nécessairement limitée, puisque c'est bien dans cet esprit que le législateur a prévu la possibilité d'ouvrir certaines de ces techniques à ces services.

En effet, sans avoir un rôle aussi central que les six services spécialisés de renseignement, dits « du premier cercle² », les autres services ayant des fonctions de renseignement doivent disposer de certaines techniques, au regard de leur rôle en matière de renseignement.

¹ Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure

² Direction générale du renseignement extérieur (DGSE), direction générale du renseignement intérieur (DGSI), direction de protection et de la sécurité de la défense (DPSD), direction du renseignement militaire (DRM), direction nationale du renseignement et des enquêtes douanières (DNRED) et TRACFIN.

Ainsi, dans le rapport n° 460 (2014-2015) au nom de la commission des lois du Sénat sur la loi relative au renseignement, il avait été précisé que « *cette disposition [la possibilité de désigner des services autres que ceux du second cercle pouvant bénéficier des techniques de renseignement] permettra à ces services, qui sans appartenir à la communauté du renseignement, exercent des missions de renseignement et intégrerait ainsi un « deuxième cercle » à l’instar de la direction du renseignement de la préfecture de police de Paris (DRPP) ou du service central du renseignement territorial (SCRT) »¹.*

La DPR s’étonne donc que le décret du 11 décembre 2015 précité ait retenu une définition **très large** des services autorisés à recourir à des techniques de renseignement (*voir Annexe 6*), ce qui pose plusieurs difficultés. En effet, les services désignés dépassent très largement le périmètre des services de renseignement du « deuxième cercle », alors qu’il est considéré qu’il rassemble surtout **la direction du renseignement de la préfecture de police de Paris (DRPP), le service central du renseignement territorial (SCRT) et la sous-direction de l’anticipation opérationnelle**, qui dépend de la gendarmerie nationale (SDAO).

En outre, l’attribution des techniques de renseignement à ces services s’est faite de manière **très large** (*voir Annexe 2*).

2. Le risque d’un contournement des procédures applicables dans un cadre judiciaire

Autoriser certaines techniques de renseignement au bénéfice de services relevant de la direction centrale de la police judiciaire ou de la direction générale de la gendarmerie nationale ayant une mission principale de police judiciaire ne présente pas en soi une difficulté, mais leur autoriser l’utilisation de techniques très intrusives, dont ils bénéficient en police judiciaire, fait courir le risque d’une confusion entre les missions relevant de la police administrative et celles relevant de la police judiciaire. En effet, ces services pourraient recourir à l’utilisation de techniques de renseignement à l’appui d’investigations menées dans un cadre judiciaire.

Ainsi, l’attribution des techniques d’accès à un système informatique ou d’intrusion domiciliaire à la sous-direction antiterroriste (SDAT)² ou à la sous-direction de la lutte contre la cybercriminalité (SDLC)³, ou à la direction de la police judiciaire⁴ est contestable. De même, a été accordée à l’OCRIEST⁵, qui dépend de la direction centrale de la police aux frontières, la technique de captation des données informatiques.

¹ Rapport n° 460 (2014-2015) fait au nom de la commission des lois, pages 43 et 44.

² Cette sous-direction relève de la direction centrale de la police judiciaire.

³ Cette sous-direction relève de la direction centrale de la police judiciaire.

⁴ Cette direction relève de la direction des opérations et de l’emploi de la direction générale de la gendarmerie nationale.

⁵ Office central pour la répression de l’immigration irrégulière et l’emploi d’étrangers sans titre.

L'exemple des données informatiques est à cet égard très éclairant. Ces données, très intrusives, présentent aujourd'hui un enjeu essentiel pour les services de police. Les garanties qui entourent l'accès à ces données **dans le cadre de la police judiciaire**, sont fortes : l'accès à un système informatique est assimilé à une **perquisition** par l'article 57-1 du code de procédure pénale et l'accès aux flux informatiques est régi par les dispositions de l'article 706-102-1 du code de procédure pénale, qui n'a été que très rarement mis en œuvre¹.

***.

Il aurait été donc préférable d'opérer les modifications nécessaires du code de procédure pénale, ce qui permettrait de **résoudre les difficultés de mise en œuvre de certaines techniques dans le cadre de la police judiciaire - en particulier l'accès aux flux informatiques² - plutôt que de développer les pouvoirs administratifs de services ayant principalement une vocation de police judiciaire.**

3. Le risque d'affecter l'efficacité des services de renseignement du premier cercle

La **crédibilité de l'action des services de renseignement** est un élément essentiel ***. Elle est conditionnée par le **nombre limité de services effectuant des tâches de renseignement** et par leur professionnalisme.

Les services du second cercle ayant une stricte mission de renseignement, soit le SCRT, la DRPP et la SDAO, disposent de la **quasi-totalité des techniques nouvelles autorisées par la loi pour les services du premier cercle**, à l'exception des techniques de suivi en temps réel des personnes préalablement identifiées comme présentant une menace (L. 851-2) et de l'algorithme (L. 851-3)³. Autrement dit, à l'exception du partage d'information renforcé permis par l'appartenance au premier cercle, **peu d'éléments les distinguent désormais des services du premier cercle.**

En outre, l'attribution de techniques délicates à mettre en œuvre à des services ne disposant pas toujours des compétences techniques requises - au-delà des services de renseignement du « deuxième cercle », beaucoup de services bénéficient des techniques -, sans leur imposer de recourir à des services spécialisés pour les installer, fait également courir le risque d'erreurs dans leur mise en œuvre, qui affecteront alors l'activité des services de renseignement, en particulier ceux du premier cercle.

¹ En effet, le passage préalable devant une commission administrative pour autoriser les logiciels entraîne des délais tels que ce dispositif n'a été mis en œuvre que six fois depuis 2011.

² Comme le propose notamment la proposition de loi tendant à renforcer l'efficacité de la lutte antiterroriste déposée le 17 décembre 2015 au Sénat.

³ Très compliquées à mettre en œuvre et nécessitant une centralisation, ces techniques ne pourraient être mises en œuvre que par un service. Actuellement, aucun de ces deux instruments n'est mis en œuvre (voir supra).

Enfin, certains choix sont particulièrement curieux : **la possibilité pour l'unité de coordination de la lutte antiterroriste (UCLAT) de recourir aux techniques de renseignement**, alors même que le rôle premier de cette unité aux effectifs modestes est de **coordonner** l'action des services en matière de lutte anti-terroriste et non de mener des investigations particulières est injustifiée, étant d'ailleurs observé que les capacités de coordination de la lutte anti-terroriste de ce service sont perfectibles.

La DPR recommande aux ministres concernés et à leurs délégués une vigilance particulière lorsqu'ils seront amenés à examiner les demandes des services dont le renseignement ne constitue pas la spécialité et de vérifier s'ils disposent des compétences techniques requises et s'ils ont mis en place des dispositifs de contrôle interne rigoureux. Elle demande au Premier ministre et à ses délégués d'assurer un contrôle vigilant lorsqu'ils devront procéder à l'examen des demandes présentées (Proposition n°6).

4. Les effets mécaniques d'une telle extension sur les organes de traitement (GIC) ou de contrôle (CNCTR)

Enfin, une telle extension entraînera mécaniquement un volume de demandes important à traiter, par les services des ministères mais aussi par le Groupement interministériel de contrôle (GIC) ou par la CNCTR.

Ainsi, sans un filtrage mené à l'échelon des ministères, la qualité et l'effectivité du contrôle exercé pourraient être fortement affectées au regard du volume de demandes à traiter.

Ce changement nécessite donc la réaffirmation du principe de centralisation ainsi qu'un contrôle approfondi et scrupuleux des procédures, selon des procédures de contrôle interne, pour vérifier notamment que l'intégralité des données, sans aucune altération, sont transmises aux organes de contrôle. ***. Le choix d'une large extension fait par le décret précité rendra ainsi d'autant plus compliquée la mise en œuvre du contrôle.

Par ailleurs, des procédures de contrôle très rigoureuses doivent être rapidement instaurées au sein des services bénéficiant de ces techniques de renseignement (voir *infra*).

C. LA NÉCESSITÉ DE METTRE EN PLACE DES PROCÉDURES DE CONTRÔLES COMPLÉMENTAIRES POUR S'ASSURER DU RESPECT DES DISPOSITIONS LÉGALES APPLICABLES

1. L'audit interne : un dispositif nécessaire mais insuffisant sans un audit externe robuste et permanent des procédures

***, le **contrôle interne des services utilisateurs** des nouvelles techniques de renseignement se pose avec acuité. Dans son rapport pour l'année 2014, la délégation avait déjà recommandé de développer le contrôle interne administratif. Les exemples de la DGSE et de la DGSII avaient été salués par la délégation qui avait recommandé de **systematiser ces procédures dans les autres services spécialisés de renseignement**¹.

a) Un contrôle interne rendu indispensable par la collecte décentralisée des renseignements

En effet, comme évoqué *supra*, les nouvelles techniques sont mises en œuvre à partir de l'enquêteur, qui collecte les données et les exploite lui-même, directement. Ce n'est donc que dans un second temps qu'il les transmet à l'organe de contrôle. Se pose donc la question nouvelle de la **non-altération du renseignement** transféré aux organismes de contrôle.

Si les évolutions techniques peuvent permettre certaines garanties - en empêchant par exemple d'effacer ou de modifier une donnée collectée, en traçant l'utilisation d'un dispositif *, celles-ci sont insuffisantes sans un mécanisme de contrôle interne renforcé, à toutes les étapes de collecte des renseignements et de leur transmission par les services utilisateurs.**

L'efficacité d'un contrôle interne repose enfin sur son évaluation très régulière, aussi bien par la hiérarchie que par des services d'audit extérieurs aux services, vérifiant scrupuleusement le respect des procédures et des démarches prescrites et se traduisant, le cas échéant, par des contrôles complémentaires à court terme pour vérifier la mise en œuvre des actions correctives préconisées.

La DPR demande la mise en place d'un contrôle administratif renforcé au sein des services de renseignement et au sein des services habilités à utiliser les nouvelles techniques de renseignement par le décret du 11 décembre 2015 (*Proposition n°7*).

¹ Recommandation n° 5, p. 70.

b) La nécessité d'un contrôle interne robuste et standardisé au sein des services du « deuxième cercle »

Dans les services du « deuxième cercle », qui bénéficient désormais pour certains de nombreuses techniques du renseignement ^{***}, la nécessité de développer un contrôle interne sur l'utilisation de ces techniques se pose avec d'autant plus d'acuité.

Traditionnellement, les services spécialisés de renseignement ainsi que des services opérant dans un cadre de police administrative, par exemple en matière de lutte contre la grande criminalité, bénéficiaient des techniques du renseignement. Désormais, ces techniques sont étendues à des services ayant principalement des missions de police judiciaire. Comme pour la DGSI, qui dispose d'une compétence de police judiciaire, une séparation claire des activités devra être garantie.

Au regard du nombre de services concernés, il conviendrait donc de **systematiser le contrôle interne**, selon un **standard commun**, afin de faciliter le contrôle externe. En effet, au regard du nombre de services bénéficiant de ces techniques, y compris parfois de leurs nombreux services décentralisés, une méthode d'évaluation commune des procédures devra être rapidement élaborée.

La DPR demande que l'inspection du renseignement propose dans les meilleurs délais un standard commun de contrôle interne (Proposition n°8).

2. La mise en place d'une inspection des services de renseignement pérenne pour permettre un audit régulier du contrôle interne

^{***}propose de faire valider les dispositifs de contrôle interne par le GIC ou par la CNCTR.

Toutefois, il ne semble pas que faire valider les processus internes par l'instance de contrôle et d'autorisation de mise en œuvre des services soit une option qui puisse être retenue. En effet, pour permettre un contrôle externe en toute indépendance, il semble préférable de ne pas impliquer ces organes - du moins la CNCTR - dans la phase de contrôle interne, au risque de lier son appréciation lors de l'examen des demandes au seul respect des procédures internes qu'elle aura préalablement avalisées.

L'envoi du schéma de contrôle interne à la CNCTR comme au GIC est toutefois nécessaire.

L'exigence d'un contrôle interne pourrait en revanche être effectuée sous la responsabilité de **l'inspection du renseignement**. Toutefois, le

dispositif actuel nécessiterait d'être fortement renforcé, pour permettre un contrôle plus effectif (*voir également Chapitre IV infra*).

En effet, si la constitution d'équipes *ad hoc* apporte une véritable plus-value, puisqu'elle permet d'associer des inspecteurs généraux de l'administration, des finances, du contrôle général des armées notamment, le programme de contrôle nécessaire pour garantir la mise en place rapide de véritables procédures de contrôles internes, faisant l'objet d'audits réguliers et effectifs nécessite la mise en place d'une **inspection propre au renseignement, pérenne** ainsi que d'un chef de l'inspection permanent, comme l'avait recommandé la délégation¹.

Au sein de l'inspection des services de renseignement, deux instances pourraient être distinguées : une première instance serait consacrée à **l'audit des procédures de contrôle interne**, permettant de vérifier régulièrement l'ensemble des services concernés selon une périodicité à définir, sans préjudice de contrôles aléatoires. Le second ensemble mènerait des **inspections**, selon le schéma actuel, en rassemblant des inspecteurs de plusieurs ministères, afin d'analyser des sujets plus généraux, comme une inspection de ministérielle ou interministérielle classique.

Comme les services audités relèveraient de plusieurs ministères, le **rattachement au SGDSN** de l'inspection du renseignement*** semble être la plus à même de permettre un contrôle efficace.

La DPR demande le renforcement et la pérennisation, dès 2016, de l'inspection des services de renseignement. Elle serait rattachée au SDGSN et pourrait comprendre deux instances, la première permanente consacrée à l'audit des procédures de contrôle interne et la seconde, rassemblant des inspecteurs de plusieurs ministères afin d'analyser des sujets plus généraux (*Proposition n°9*).

IV. LES PROPOSITIONS DE LA DPR

1/ Affecter au GIC les personnels mis à disposition par le ministère de la défense avant le 31 décembre 2017.

2/ Attribuer au GIC le statut de service à compétence nationale.

3/ Rendre l'arbitrage technique * dans les meilleurs délais.**

4/ Mettre en œuvre sans retard les techniques de renseignement * eu égard *** au niveau de la menace terroriste.**

¹ Recommandation n° 6 du chapitre IV.

5/ Permettre à la CNCTR de disposer d'un accès permanent, complet et direct aux éléments collectés par les nouvelles techniques dans les conditions posées par la loi et dans des délais raisonnables.

6/ Exercer un contrôle vigilant sur les demandes des services habilités à utiliser les nouvelles techniques de renseignement par le décret du 11 décembre 2015 dont le renseignement ne constitue pas la spécialité. La DPR recommande aux ministres concernés et à leurs délégués une vigilance particulière lorsqu'ils seront amenés à examiner ces demandes, de vérifier s'ils disposent des compétences techniques requises et s'ils ont mis en place des dispositifs de contrôle interne rigoureux. Il demande au Premier ministre et à ses délégués d'assurer un contrôle vigilant lorsqu'ils devront procéder à l'examen des demandes présentées.

7/ Mettre en place d'un contrôle administratif renforcé au sein des services de renseignement et au sein des services habilités à utiliser les nouvelles techniques de renseignement par le décret du 11 décembre 2015.

8/ Demander à l'inspection des services de renseignement de proposer dans les meilleurs délais un standard commun de contrôle interne.

9/ Renforcer et pérenniser, dès 2016, l'inspection des services de renseignement. Elle pourrait comprendre deux instances, la première permanente consacrée à l'audit des procédures de contrôle interne et la seconde, rassemblant des inspecteurs de plusieurs ministères afin d'analyser des sujets plus généraux. Elle serait rattachée au SGDSN.

CHAPITRE III : LA SURVEILLANCE INTERNATIONALE

Par les informations qu'elle recueille et les analyses dont elle permet l'élaboration, la surveillance internationale garantit l'autonomie d'appréciation des plus hautes autorités de l'État dans la prise de décisions stratégiques et, par voie de conséquence, la souveraineté de l'État. Elle apporte une contribution essentielle à la politique de sécurité intérieure et extérieure.

La surveillance internationale est un concept dont la définition a été fluctuante. Il a pu s'agir de la surveillance des activités conduites par des ressortissants étrangers ou pour le compte de puissances étrangères qu'elle se déroule sur le territoire national ou à l'étranger. Il a pu également s'agir de la surveillance des activités qui se déroulent hors du territoire national que celle-ci soit réalisée depuis le territoire national ou à l'extérieur de celui-ci. C'est cette dernière définition qui a été retenue par l'article L. 854-1 du code de sécurité intérieure, inséré par la loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales¹.

L'existence et le maintien de capacités de surveillance internationale efficaces constituent un outil stratégique indispensable à la sauvegarde des intérêts fondamentaux de la France.

Le Gouvernement doit veiller par des orientations et des choix appropriés à ce que cet outil puisse répondre aux besoins, conserve et améliore son efficacité et s'adapte tant à l'évolution des menaces qu'à celles des technologies de l'information, de l'observation et de la communication ainsi que de leurs usages. Il doit veiller à maintenir à un niveau opérationnel élevé les différentes sources dont les apports contribuent à la qualité de l'information : renseignement d'origine humaine, renseignement technique, renseignement partenarial en développant un niveau d'expertise élevé, en adaptant ses méthodes et en investissant dans de nouvelles technologies de captation.

I. LA SURVEILLANCE INTERNATIONALE A L'ÉPREUVE DE L'ORGANISATION

La surveillance internationale repose principalement sur deux services spécialisés de renseignement : la DGSE et la DRM.

Comme l'ensemble des services spécialisés de renseignement, ces deux services réalisent des actions de surveillance internationale, notamment des communications électroniques, mais ils assurent en outre au profit de

¹ Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

l'ensemble de la communauté du renseignement, la mise à disposition de plateformes techniques permettant la réalisation de ces opérations. Ces deux services relèvent du ministère de la défense.

A. UN SERVICE SPÉCIALISÉ DANS LE RENSEIGNEMENT EXTÉRIEUR : LA DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE (DGSE)

1. Statut

La DGSE a été créée par un décret du 2 avril 1982, transposé dans les articles D. 3126-1 à D.3126-4 du code de la défense. Son organisation interne est fixée par l'arrêté du 21 décembre 2012.

2. Missions

Le champ d'action de la DGSE se situe essentiellement hors des frontières, elle y applique des méthodes clandestines de recherche du renseignement. Le secret des moyens employés et des objectifs poursuivis garantit la sécurité de la DGSE et de ses agents.

Sa mission est de rechercher à l'étranger des informations secrètes, intéressant la défense et la sécurité nationales (renseignement de crise, contre-terrorisme, contre-prolifération, *** notamment). En communiquant aux autorités les éléments ainsi recueillis et analysés, elle participe à leur prise de décision.

La DGSE est présente dans les zones de crise et partout où les intérêts français sont en jeu.

Elle permet le maintien d'une présence, là où les canaux diplomatiques ne peuvent plus être utilisés.

Service de renseignement intégré, elle maîtrise la totalité des modes de recueil de renseignements : sources humaines, capteurs techniques (interceptions électromagnétiques et imagerie satellitaire¹ principalement), moyens opérationnels et sources ouvertes.

Elle obtient également des renseignements par le biais de coopérations avec d'autres services, français et étrangers. Enfin, la DGSE dispose d'une capacité d'entrave et d'action ***.

¹ Via la DRM qui exerce le contrôle opérationnel des capteurs optiques et les armées le commandement opérationnel des satellites.

3. Organisation

Outre les structures placées sous l'autorité directe du directeur général, la DGSE comprend la direction du renseignement, la direction de l'administration, la direction technique, la direction des opérations et la direction de la stratégie.

Elle dispose également d'un certain nombre de postes à l'étranger dont le réseau a été resserré pour tenir compte des intérêts et des menaces autour de l'Afrique du Nord, du Moyen-Orient, de l'Afrique de l'Ouest et de l'Afrique centrale et enfin de certaines grandes puissances. Elle peut également mettre en place des missions temporaires chargées d'animer des réseaux de correspondants locaux ou de conduire des opérations spécifiques.

4. Ressources humaines

La répartition des emplois du ministère de la défense par gestionnaire fait apparaître au sein du programme 212, un plafond d'emplois de 5 302 équivalents temps plein travaillés pour la DGSE au 1^{er} janvier 2015 qui se traduisent, de fait pour le service, en termes d'effectifs réels à 5 072 équivalents temps plein emplois au 30 juin 2015 et un effectif attendu au 31 décembre 2015 de 5 208. Elle bénéficie de renforcement d'effectif sur la période de la loi de programmation militaire 2014-2019 à hauteur de *** créations qui intègrent celles obtenues lors de la loi de programmation initiale (***), celles qui résultent d'une décision du Premier ministre à la suite des attentats de janvier 2015 (***), et celles obtenues dans le cadre de l'actualisation de la LPM en juillet 2015 (**) puis à l'issue des attentats de novembre 2015 (**). ** créations ont été réalisées en 2014, ** en 2015, le solde devrait s'échelonner jusqu'en 2019, à raison de ** créations en 2016, ** en 2017, ** en 2018 et ** en 2019.**

On observe une progression des emplois de catégorie A ou officiers, une érosion régulière du personnel militaire (sous-officier notamment) et une part croissante de contractuels parmi les personnels civils, corollaire de la diversification des profils recherchés (notamment dans les spécialités linguistiques, scientifiques et techniques).

5. Moyens budgétaires

La DGSE disposera d'un budget annuel ** de plus de 700 millions d'euros en CP en 2016. Les crédits se répartissent ainsi :

- au titre 2 du programme 212 de la mission « Défense » dans la sous-action « Renseignement extérieur » pour ce qui concerne les

rémunérations des personnels civils et militaires *** pour un montant de 412,89 millions d'euros en 2016 ***.

- hors titre 2 au programme 144 de la mission « Défense » (sous-action : « Renseignement extérieur ») pour ce qui concerne les crédits de fonctionnement, d'équipements et d'interventions de la direction générale pour un montant de 224,26 millions d'euros en CP et 237,26 en AE¹.

S'y ajoutent :

- des crédits inscrits à l'action 02 du programme 129 « Coordination de l'action gouvernementale » au titre des « capacités techniques interministérielles » (CTIM) qui sont transférés par décret en cours d'année² et une partie de la dotation en fonds spéciaux dont le contrôle est effectué par la CVFS³.

Enfin, certaines dépenses d'équipement correspondant à des programmes d'armement pilotés par la Direction générale de l'armement (DGA) relèvent du programme 146.

B. UN SERVICE SPÉCIALISÉ DANS LE RENSEIGNEMENT MILITAIRE : LA DIRECTION DU RENSEIGNEMENT MILITAIRE (DRM)

1. Statut

Créée par décret du 16 juin 1992 (transposé dans le code de la défense aux articles D. 3126-10 à D. 3126 -14), la DRM a vu son organisation et son fonctionnement fixés par l'arrêté du 16 février 2010 modifié.

2. Missions

La DRM est chargée de renseigner les autorités politiques et militaires et de les aider dans leurs choix, au titre de la veille stratégique des risques et menaces. Elle doit également fournir au chef d'état-major des armées, le renseignement nécessaire pour proposer les options militaires et conduire les opérations sur les théâtres.

Dans ce cadre, sa mission est donc de recueillir et d'élaborer du renseignement d'intérêt militaire, c'est-à-dire tout ce qui a ou peut avoir des

¹ ***

² ***

³ Le montant total des crédits de fonds spéciaux inscrits dans le PLF 2016 est de 47,53 millions d'euros. ***

conséquences sur les forces en opérations dans les crises actuelles ou potentielles.

Le directeur du renseignement militaire assiste et conseille également le ministre de la défense en matière de renseignement d'intérêt militaire.

Service de renseignement autonome, la DRM dispose en propre de la totalité des modes de recueil du renseignement : imagerie satellitaire, interceptions électromagnétiques, recherche humaine, informatique.

Les armées peuvent mettre à sa disposition d'autres capteurs afin de compléter cette palette. Elle obtient également du renseignement grâce à ses partenaires internationaux.

Elle élabore le renseignement nécessaire à l'appréciation autonome de situation et à la conduite des opérations, qu'elle diffuse aux autorités politiques et aux chefs militaires.

3. Organisation

La DRM relève du chef d'état-major des armées. Elle est constituée d'un échelon de direction, de trois sous-directions (sous-direction des opérations, sous-direction de l'exploitation, et sous-direction personnel, finances, capacités) et d'un bureau renseignement au centre de planification et de conduite des opérations (CPCO).

Quatre centres spécialisés lui sont rattachés : le centre de formation et d'emploi relatif aux émissions électromagnétiques (CF3E), le centre de formation et d'interprétation interarmées de l'imagerie (CF3I), le centre interarmées de recherche et de recueil du renseignement humain (CI3RH) et le centre de formation interarmées au renseignement (CFIAR).

Elle a engagé depuis mai 2014, une transformation profonde de son organisation et de son fonctionnement avec la création :

- deux nouveaux centres *high tech* (CRGI, Centre de renseignement géospatial interarmées ; CRAC, Centre de recherche et d'analyse cybernétique) ;

- trois plateaux intégrés (tous métiers et experts réunis par thématiques) pour chaque théâtre d'opérations ;

- deux structures transverses pour éviter tout cloisonnement : un pôle stratégie et un centre de commandement chargé d'accélérer les processus.

4. Ressources humaines

La DRM dispose d'un effectif de 1 600 personnes (**% de militaires et **% de civils). Dans le cadre de l'actualisation de la loi de programmation militaire 2014-2019, ses effectifs vont être renforcés : ainsi, ** ETPT sont prévus pour 2018.

5. Moyens budgétaires

Les moyens budgétaires de la DRM sont retranscrits, s'agissant de la rémunération des personnels à la sous-action « Renseignement d'intérêt militaire » au sein du titre 2 du programme 212 de la mission « Défense » pour un montant de 136,934 millions d'euros en PLF 2016 (contre 127,528 millions en 2015) et pour ce qui concerne les crédits de fonctionnement et de maintien en condition opérationnelle au sein du programme 178 à hauteur de 36,309 millions d'euros en CP¹ et 36,856 en AE.

Certains grands équipements qui font l'objet de programmes d'armement pilotés par la DGA sont financés sur le programme 146.

Le budget de la DRM est donc réparti en trois programmes dont elle n'a pas la totale maîtrise.

C. LES QUATRE AUTRES SERVICES SPÉCIALISÉS ONT DES ACTIVITÉS INTERNATIONALES PLUS RÉDUITES

1. La DNRED

La Direction nationale du renseignement et des enquêtes douanières (DNRED) a pour mission de lutter contre les grands trafics en démantelant les organisations criminelles qui se livrent à la contrebande d'armes, de stupéfiants, de tabac et de produits contrefaits, portant atteinte au commerce légal et présentant des risques pour la santé publique.

Son action s'articule essentiellement autour de trois axes :

- la lutte contre les grands courants de contrebande ;
- la mise en œuvre des enquêtes anti-fraude d'envergure nationale et internationale diligentées à l'encontre des entreprises et des particuliers ;
- la gestion et l'animation de la collecte du renseignement, son traitement et sa diffusion, à l'ensemble des services douaniers ainsi qu'aux services partenaires.

¹ **

Elle s'appuie sur son analyse des flux de marchandises et de personnes, sur le recueil de renseignements opérationnels ainsi que sur la mise en œuvre de certaines techniques spécialisées d'investigation. Elle exerce son activité sur l'ensemble du territoire douanier national. Elle coordonne également les activités opérationnelles du réseau des attachés douaniers français qui couvre près de 60 pays.

Dans le cadre de son activité, la DNRED utilise les moyens de la surveillance internationale et est également un contributeur important pour la communauté des services, en matière de lutte contre le crime organisé, mais également dans la lutte contre le terrorisme dont les activités illégales de trafic assurent une part importante du financement et qui s'approvisionne en armement auprès de trafiquants. Elle participe à la plupart des cellules interservices mises en place à cette fin.

2. TRACFIN

TRACFIN a pour mission de lutter contre les circuits financiers clandestins, le blanchiment de l'argent et le financement du terrorisme.

À partir des déclarations effectuées par les professionnels assujettis au dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme ou d'informations reçues des services homologues étrangers, la cellule recueille, analyse, enrichit et exploite tout renseignement propre à établir l'origine ou la destination délictueuse d'une opération financière.

Sa culture intrinsèque, l'oriente vers l'exploitation de sources ouvertes. Pour ce qui concerne la lutte contre le terrorisme qui s'appuie sur des circuits financiers qui lui sont propres, elle pourrait s'appuyer davantage à l'avenir sur les techniques de renseignement existantes, y compris à l'international.

3. La DPSD

La Direction de la protection et de la sécurité de la défense exerce une mission de contre-ingérence au profit du ministère de la Défense et des entreprises de défense. Si sa mission est principalement orientée sur la protection du secret, des sites sensibles et du personnel de la défense ainsi que sur la sécurité économique au profit des entreprises de défense, elle exerce une partie de ses missions sur les théâtres extérieurs où les armées sont engagées. Dans ces différentes activités et notamment dans l'exercice de cette dernière, elle recueille du renseignement de contre-ingérence et contribue dans son domaine à la surveillance internationale. De même, elle est susceptible de solliciter l'utilisation des moyens déployés par d'autres services, en propre ou en interministériel, pour recueillir du renseignement dans le cadre de l'exercice de ses missions.

4. La DGSI

Créée par décret du 30 avril 2014, la direction générale de la sécurité intérieure a pour mission de lutter contre les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la Nation. Elle est chargée de prévenir et de réprimer, sur le territoire national, les activités inspirées, engagées ou soutenues par des puissances ou des organisations étrangères et de nature à menacer la sécurité du pays.

Ses activités s'articulent autour de cinq pôles : le contre-espionnage, la contre-ingérence économique, la contre-prolifération, la lutte contre le terrorisme et les extrémismes violents ainsi que la lutte contre la grande criminalité organisée et la cyber criminalité.

Si elle exerce ses missions essentiellement sur le territoire national¹, la DGSI est un pourvoyeur de renseignements utiles pour la surveillance internationale, notamment dans le cadre d'activités qui s'affranchissent aisément des frontières, comme elle est un utilisateur des outils de surveillance internationale déployés par d'autres services spécialisés ou développés en interministériel. Cette collaboration étroite avec les autres services s'est particulièrement développée avec la montée en puissance de la lutte contre le terrorisme, d'autant que celui-ci s'appuie pour partie sur des combattants français ou résidents en France, ayant subi une formation à l'étranger. Elle a été facilitée par la nomination parmi ses plus hauts cadres de fonctionnaires ayant effectué une mobilité extérieure au sein de la DGSE, ce qui permet un travail collaboratif plus fluide.

D. LE CHOIX DE LA SPÉCIALISATION ET DE LA MUTUALISATION

Le renseignement technique a pris une place quantitativement croissante dans les sources de renseignement, au fur et à mesure du développement des technologies de l'information, de la communication et l'imagerie.

La spécialisation des services de renseignement a conduit à doter chacun d'entre eux de capacités propres. Néanmoins, l'émergence du renseignement technique a conduit l'État à s'engager dans un processus de **mutualisation des moyens techniques** pour éviter de coûteuses duplications mais aussi dans le but de les superviser. ***

La France n'a pas opté pour la mise en place d'une agence technique, gestionnaire de l'ensemble des moyens et pourvoyeuse des différents services spécialisés, ce qui a été le choix des États-Unis et de la Grande-Bretagne.

¹ La DGSI dispose néanmoins de *** postes à l'étranger distincts du réseau de la coopération internationale de la DGPN.

Les deux solutions ont leurs avantages et leurs inconvénients. A l'heure où l'imbrication des menaces est forte (grande criminalité/terrorisme, continuum territoire national/théâtres d'opération extérieurs, continuum défense/sécurité intérieure), certains s'interrogent sur la pertinence de l'organisation choisie.

Alors que nos services sont mobilisés de façon intense dans la lutte contre le terrorisme, il n'est sans doute pas raisonnable d'entrer dans la voie d'une réorganisation qui, dans un premier temps, risque de mobiliser les énergies et d'affaiblir les 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 de l'architecture d'ensemble.

La DPR recommande que les dispositifs collaboratifs et coopératifs mis en place par les services fassent l'objet de retours d'expérience réguliers, pour en améliorer le fonctionnement et à terme servir de base à une réflexion sur une éventuelle réorganisation. L'organisation du recueil de ces retours d'expérience pourrait être confiée au CNR, en s'appuyant au besoin sur la définition d'une méthodologie d'évaluation préparée par l'inspection des services de renseignement (*Proposition n°10*).

II. LA SURVEILLANCE INTERNATIONALE À L'ÉPREUVE DES TECHNOLOGIES

La surveillance internationale repose sur l'emploi de **trois grandes catégories de capteurs (électromagnétiques, images, humains)**. ***

Devant la multiplicité des capteurs, la profusion des informations collectées, l'enjeu est désormais celui de la sélection, de l'intégration de l'enrichissement et de l'analyse. Il s'agit là d'un enjeu d'organisation.

Il est aussi dans le maintien au plus haut niveau de la technologie mise en œuvre pour capter et exploiter, ce qui suppose **un effort permanent d'investissement**. Dans son précédent rapport, la délégation avait souligné l'importance de poursuivre ces investissements afin que notre pays conserve son autonomie stratégique et, par ce biais, les intérêts fondamentaux de la Nation et conserver ainsi la maîtrise technologique et la capacité de production des composants électroniques nécessaires à la fabrication d'outils informatiques sensibles¹.

¹ Délégation parlementaire au renseignement, Rapport d'activité 2014, contrôler les services de renseignement - An I, n° 2482 (Assemblée nationale) et 201 (Sénat). Proposition n° 2 du chapitre VII.

A. LA SURVEILLANCE DES COMMUNICATIONS (RENSEIGNEMENT D'ORIGINE ÉLECTROMAGNÉTIQUE - ROEM)

Historiquement, les communications militaires utilisaient essentiellement la voie hertzienne à raison de la mobilité des forces et de la facilité de déploiement des réseaux. La surveillance internationale s'est donc appuyée, de longue date, sur des moyens de captation des communications utilisant les fréquences hertziennes, y compris transitant par des satellites.

L'arrivée du haut-débit, la croissance exponentielle des échanges de données et le développement de l'Internet ont conduit au déploiement des réseaux physiques en fibre optique dont les capacités sont infiniment plus grandes que le spectre hertzien. 99 % du trafic international de téléphone et de données passent par le million de kilomètres de câbles sous-marins – 340 réseaux reliant tous les continents. Leur fiabilité, leur sécurité et leur faible coût comparé aux liaisons satellites en font des infrastructures décisives de la « globalisation ».

Les services de renseignement des principales puissances ont développé des outils permettant d'assurer la captation d'une partie des communications internationales aux fins d'assurer la sauvegarde de leurs intérêts fondamentaux.

La DPR recommande * (*Proposition n°11*)**

La DPR recommande * (*Proposition n°12*).**

(1) ***

(2) Les capacités spatiales de renseignement électromagnétique

Plusieurs développements expérimentaux ont été réalisés¹. Le programme CERES, lancé en 2007, vise à disposer d'une capacité opérationnelle d'écoute susceptible d'intercepter et de localiser des émissions électromagnétiques depuis l'espace. Le coût de ce système est évalué à 460 millions d'euros².

*** la phase de réalisation a démarré en janvier 2015 pour une mise en service opérationnelle prévue en 2020.

1 ***

2 ***

Compte tenu ***, la DPR estime qu'un mode d'évaluation *** devrait être mis en place et que ces données devraient figurer dans le rapport d'activité des services qui lui est transmis chaque année (*Proposition n°13*).

La DPR recommande *** (*Proposition n°14*).

La DPR recommande qu'une étude *** (*Proposition n°15*).
La DPR recommande que le CNR s'assure ***. (*Proposition n°16*).

B. L'OBSERVATION (SATELLITES, AVIONS, DRONES, NAVIRES)

Pour recueillir le renseignement d'origine image, la DRM s'appuie sur ses moyens propres, ceux des capteurs aériens des armées et ceux de ses alliées.

1. Les satellites d'observation

a) Les moyens actuels

Elle exerce par délégation du CEMA le contrôle opérationnel des deux satellites *Hélios 2* *** le seul système militaire d'observation spatiale optique en opération en Europe, et de la constellation *Pléiades* (haute résolution et images couleurs)¹.

Elle bénéficie également d'un droit de tirage sur les satellites radars allemands (*Sar Lupe*)² et italiens (*Cosmos SkyMed*)³ via le segment sol d'observation *PHAROS*⁴. En contrepartie des droits de programmation qu'elle a négociés sur les satellites italiens et allemands, la France a concédé des possibilités analogues pour ces deux pays sur les satellites *Hélios 2*.

b) Les moyens futurs

Les programmes d'investissement en cours vont permettre d'avoir accès à un flux d'images considérablement multiplié ***.

- Il s'agit du programme *MUSIS*⁵ qui a pour objectif la réalisation du futur système européen d'observation spatiale militaire, intégrant des capacités optique et radar. Ce système devrait remplacer, à terme l'ensemble

1 ***

2 ***

3 ***

4 ***

5 ***

des composantes *** opérationnelles susmentionnées. Il améliorera les performances actuelles par une meilleure résolution ***. En l'absence d'accord de coopération finalisé, et afin d'éviter tout risque de rupture capacitaire, en 2010, la France a lancé la réalisation d'un segment sol minimum ouvert à la coopération, et une partie de la composante optique (2 satellites CSO 1 et 2 sur 3)¹ pour un coût économique de 1,4 milliard d'euros (2012) auquel s'ajoute un coût de maintien en condition opérationnelle de 0,4 milliard sur 12 ans.

Le conseil des ministres franco-allemand de Berlin le 31 mars 2015 a décidé de mettre en place une coopération entre le futur système allemand d'observation radar par satellite SARah² et le système spatial optique en cours de réalisation sous responsabilité française. L'accord comprend, pour la France, l'acquisition d'un segment sol du système SARah, et pour l'Allemagne, l'acquisition d'un segment sol du système optique ; ces segments permettront l'échange d'images. Il prévoit également le financement par l'Allemagne, aux deux tiers (210 millions d'euros) du troisième satellite optique dont la programmation sera mise en service interviendra en 2021 après celle de CSO1 et CSO2 en 2018 et 2019 respectivement.

Cette relance de la coopération franco-allemande est satisfaisante.
--

- Mais aussi des satellites européens *COPERNICUS* et *SENTINEL*, qui offriront des taux de revisite très intéressants pour les opérations.

Alors qu'aujourd'hui, la programmation vise à répondre à une question précise, demain c'est un stock d'images qui permettra de répondre sans délai à la question grâce à des archives directement accessibles.

Pour la génération suivante, au regard des coûts croissants des programmes de satellites d'observation et des avancées technologiques en terme de miniaturisation, il faut se poser la question des nanosatellites, déployables en essais qui permettront de garantir la résilience nécessaire et d'assurer une forte répétitivité qui amplifierait la qualité du renseignement recueilli.

¹ Leur déploiement a été reporté à 2017 et 2018, échéance compatible avec la durée de vie prévisible d'Hélios2.

² Dont la mise en service opérationnelle complète est prévue à l'horizon 2020

2. Les aéronefs

a) Les avions de surveillance et de reconnaissance

La location de *** avions légers de surveillance et de reconnaissance apportent une plus-value en opérations, grâce à leur faible empreinte au sol et à leur adaptabilité en termes de capteurs ***.

La DPR prend acte de l'acquisition prochaine de * ALSR mais souhaite que cet effort soit prolongé.**

b) Les capteurs embarqués sur des aéronefs de combat et de patrouille maritime

Les armées disposent de capteurs aériens : les Rafale de l'armée de l'air et de la marine sont équipés de *pod reco NG* qui fournissent des photographies avec un excellent niveau de résolution.

En outre, les *Atlantique2* de la marine sont fréquemment employés par la DRM en dépit de leur faible disponibilité.

c) Les capteurs embarqués sur les drones

La DRM oriente également les systèmes de drones *Reaper* et *Harfang* déployés au Sahel par l'armée de l'air. Les drones MALE constituent des moyens aériens projetables, capables d'assurer des missions de renseignement, de surveillance, de reconnaissance et de désignation d'objectifs opérants, grâce à leur endurance, sur de larges zones, à grandes distances et sur de longues durées (de l'ordre de 24 heures). Ils apportent par leur durée de vol et leur discrétion, une permanence dans la surveillance et une aide décisive dans le cycle du ciblage.

Un second système *Reaper* a été commandé en juillet 2015 pour une livraison en 2016 et la commande d'un troisième système (le premier au standard Block 5) est prévue d'ici la fin de l'année 2015. La loi de programmation militaire 2014-2019 prévoit la livraison de quatre systèmes complets, comprenant chacun trois vecteurs sur la durée de la programmation.

Le système actuellement en dotation *** sert de manière intensive dans le cadre de l'opération Barkhane.

Les retours d'expériences doivent pouvoir alimenter la préparation du futur et permettre d'orienter les spécifications du futur drone MALE européen à l'horizon 2020 -2025¹. Pour être au meilleur niveau, ces systèmes

¹ La signature, le 18 mai 2015, d'une lettre d'intention entre l'Allemagne, l'Italie et la France, rejointes par l'Espagne, constitue un nouveau jalon dans cet effort de recherche. Il est prévu qu'une étude d'une durée de deux ans détermine les prérequis opérationnels puis élabore un prototype répondant à une expression de besoin commun en termes de performance, de calendrier et de coût.

devront pouvoir intégrer de la vidéo, des moyens d'écoutes des communications et de l'armement.

d) Le traitement automatisé des images

L'exploitation de l'ensemble de ces images est réalisée par le centre de formation interarmées à l'interception d'images (CF3I) implanté à Creil qui est le référent ROIM de la Défense. L'ensemble des images satellitaires, aériennes et prises au sol recueillies par les armées y est stocké. Elles seront prochainement consultables à distance. L'une des principales difficultés aujourd'hui est l'accroissement du flux des images ***.

C. LE RENSEIGNEMENT HUMAIN

Le développement des techniques de renseignement et la massification de fait de la collecte de données ont eu pour conséquence aux yeux de nombreux commentateurs, à charge ou à décharge, de réduire la place du renseignement humain.

Or, s'ils reposent sur des approches différentes, la performance des services se mesure dans leurs capacités à articuler efficacement l'ensemble des techniques dont ils disposent et à développer un niveau suffisant d'expertise.

Il est donc vain comme on le lit souvent dans la presse d'opposer le renseignement technique et le renseignement humain. L'État doit cependant veiller dans l'affectation des moyens à ce que les efforts soient réalisés pour permettre la combinaison la plus efficiente pour assurer la valeur ajoutée la plus grande en fonction des besoins exprimés.

<p>La DPR demande, en conséquence, que les efforts pour conforter les moyens du renseignement humain soient amplifiés (<i>Proposition n°17</i>).</p>

1. La DRM

a) Les capacités propres de la DRM

Les capacités propres de la DRM sont regroupées au sein du centre interarmées de recueil et de recherche du renseignement d'origine humaine. Elles sont complétées par celles des armées. Ce centre référent pour les Armées est en phase de montée en puissance.

b) L'administration de l'ensemble des sources humaines des armées

Ses missions consistent en l'administration de l'ensemble des sources humaines des armées, leur exploitation, la relation avec les entreprises et le monde civil, la coordination de la recherche humaine sur les théâtres d'opérations et dans les zones de crise.

La DRM a vocation à solliciter le réseau des attachés de défense (une centaine dans le monde).

Elle s'appuie également sur le 13^{ème} RDP qu'elle emploie sur les théâtres d'opération mais aussi au titre de l'anticipation en renfort des missions militaires.

Elle peut également s'appuyer sur les moyens du 2^{ème} RH, régiment de recherche profonde, spécialisé notamment dans la conduite des interrogations des personnes capturées et ponctuellement sur les unités du Commandement des opérations spéciales pour des missions particulières.

Les effectifs de la DRM et des armées dédiés au renseignement d'origine humaine sont de *** dont *** engagés en OPEX.

c) La centralisation et l'enrichissement du renseignement

L'enjeu actuel dans le domaine du renseignement réside dans les capacités à intégrer, enrichir et diffuser les masses d'information qui parviennent des différents capteurs pour en faire une information utile soit à la décision politique soit à l'action opérationnelle.

S'agissant du renseignement d'intérêt militaire, une fois le renseignement recueilli et exploité par les capteurs placés sous le contrôle opérationnel du bureau renseignement de l'état-major interarmées de théâtre par exemple, l'ensemble des données est transféré par liaison satellite dans chacun des centres de la DRM où il sera valorisé, archivé et exploité, puis transmis au centre de renseignement géospatial interarmées (CRGI) où il sera fusionné sur un support cartographique. Les données ainsi produites seront acheminées vers le plateau spécialisé qui regroupe les spécialistes de la recherche et les analystes compétents, qui les analysera et les enrichira de renseignements recueillis ailleurs pour produire les notes et les cartes demandées par les autorités politiques et militaires ou la force engagée sur le théâtre.

Le centre de renseignement géospatial des armées

Le CRGI est un outil de fusion multicapteurs destiné à répondre à de nouveaux enjeux en projetant toutes les couches du renseignement sur une interface géographique. Il a pour but d'agréger l'ensemble du renseignement recueillis par les capteurs et de fournir aux forces un renseignement directement utilisable.

Créé en janvier 2015, le CRGI se compose de *** personnes réparties à Creil et à Paris. Il disposera de *** experts en 2018.

2. La DGSE

Les autorités françaises ont consenti d'importants efforts dans le domaine du renseignement technique, essentiellement auprès de la DGSE. Pour autant, « *il faut éviter une excessive dépendance à l'égard du renseignement technique* » qui ne peut à lui seul donner les clés. « *Le renseignement humain est tout à fait indispensable* »¹. La DGSE a relancé de façon systématique la recherche humaine et l'analyse de façon à maintenir un équilibre satisfaisant entre ces deux pôles grâce à un double mouvement de redéploiement interne et de recrutement. Une partie importante des renforcements en effectifs *** concerneront la direction du renseignement.

a) Mission de la direction du renseignement

La direction du renseignement a pour missions le contre-espionnage, le contre-terrorisme, le renseignement politique, la contre-prolifération ***.

Elle assure l'exploitation de l'ensemble des sources techniques, humaines, opérationnelles et partenariales qui convergent vers elle. Elle met en œuvre la recherche humaine.

b) Moyens de la direction du renseignement

Elle dispose *** de ETPT², dont *** sont déployés dans les postes et *** sont chargés du suivi des postes.

*** % sont des emplois de catégorie A.

Sa montée en puissance sur la durée de la loi de programmation militaire (2014-2019) devrait permettre l'affectation de 50 % des ressources nouvelles sur la zone Irak-Syrie, sans dégrader les autres secteurs.

c) Organisation

D. LE CYBER, UN ESPACE SPÉCIFIQUE

Le cyber *** constituent une véritable mine d'informations qu'il convient d'exploiter au mieux grâce à des outils de veille internet. Le cyberspace est toutefois exposé au risque de la désinformation. De plus, la profusion des données disponibles nécessite qu'elles soient ciblées, voire le cas échéant déchiffrées. ***

- *** ce domaine est monté en puissance au sein de la DRM ***.

¹ Bernard Bajolet – intervention lors des 13^{ème} Université de la défense Strasbourg 15 septembre 2015

² ***

- Au sein de la DGSE, ***.
- La DGSi dispose également de capacités de suivi dans ce domaine. Elle est en outre engagée tant en matière de renseignement que de police judiciaire dans la lutte contre les cybermenaces.

E. LE RENSEIGNEMENT PARTENARIAL

Enfin et pour mémoire, il convient de mentionner le renseignement d'origine partenarial ***.

III. LA SURVEILLANCE INTERNATIONALE A L'ÉPREUVE DU DROIT

La surveillance internationale repose *** sur une base juridique stabilisée.

A. LES COMMUNICATIONS ÉLECTRONIQUES INTERNATIONALES UTILISANT LES RÉSEAUX PHYSIQUES

*** la surveillance des communications internationales, par sa nature même, a pour objet de surveiller des individus dont les noms sont souvent inconnus, des zones dans lesquelles agissent des groupes qui menacent notre pays ou ses intérêts, ou des organisations terroristes.

1. La nécessité de placer la surveillance dans un cadre légal de niveau législatif

Si ces capacités n'ont pas pour objet l'interception de communications échangées entre résidents français, elles n'en restent pas moins exploitées sur le territoire national et peuvent, de manière exceptionnelle, intercepter des communications entre des personnes dont les numéros ou identifiants techniques sont rattachables au territoire français.

Il est donc apparu indispensable que ces mesures de surveillance bénéficient, au même titre que les autres techniques de recueil de renseignement, d'une base juridique et d'un cadre légal définissant leurs finalités ainsi que les conditions de leur autorisation, de leur mise en œuvre et de leur contrôle.

Bien que strictement tournée vers le recueil de renseignements hors du territoire de la République, cette technique doit néanmoins s'inscrire dans le respect de notre ordre constitutionnel, le législateur ayant à ce titre

l'obligation, comme l'a rappelé le Conseil constitutionnel, de définir les règles relatives aux garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques.

2. L'insertion de dispositions dans le projet de loi relative au renseignement

Sur la base de ce raisonnement, le Gouvernement a pris la décision d'inclure des dispositions particulières dans le projet de loi relative au renseignement.

Le projet adopté par le Parlement le 24 juin 2015 proposait d'insérer, dans le nouveau livre VIII du code de la sécurité intérieure, un chapitre IV, intitulé : « *Des mesures de surveillance internationale* » qui ne contenait qu'un seul article L. 854-1, autorisant « *la surveillance et le contrôle (interception des communications et recueil des données de connexion) des communications qui sont émises ou reçues à l'étranger* », dès lors qu'elles répondent aux finalités définies par l'article 811-3 du code de la sécurité intérieure.

Ces interceptions se seraient toujours faites sur autorisation du Premier ministre ou des personnes déléguées par lui. Toutefois, la procédure serait définie par un décret en Conseil d'État pris après avis de la CNCTR. Un second décret en Conseil d'État, non publié, pris après avis de la CNCTR et porté à la connaissance de la DPR devait préciser, en tant que de besoin, les modalités de mise en œuvre.

La CNCTR assurerait une fonction de contrôle du respect des règles fixées pour la mise en œuvre de ces écoutes, de sa propre initiative ainsi qu'à celle de toute personne y ayant un intérêt direct ou personnel¹.

L'article L.854-1 prévoyait cependant que lorsque les communications interceptées renvoient à des numéros d'abonnement ou à des identifiants techniques rattachés au territoire national ou à des personnes faisant l'objet d'interceptions de sécurité sur le territoire national, seules les règles de droit commun relatives à la conservation et à la destruction des données s'appliqueraient.

Contrairement à ce que le législateur avait fait pour les mesures de surveillance nationale, l'article L. 854-1 renvoyait donc à des décrets en Conseil d'État la définition des conditions d'exploitation, de conservation et de destruction des renseignements collectés, ainsi que les conditions de traçabilité et de contrôle par la commission de la mise en œuvre des mesures de surveillance.

¹ En réalité, son contrôle devait être permanent dans la mesure où elle serait tenue d'adresser un rapport au Premier ministre au moins une fois par semestre, ce dernier devant adresser une réponse motivée aux observations et recommandations, dans un délai de 15 jours après réception de ce rapport.

3. Ces dispositions ont été jugés insuffisantes par le Conseil constitutionnel

Le Conseil constitutionnel¹ a estimé « *qu'en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* ».

Il en a conclu que les dispositions du 1er alinéa de l'article L.854-1, qui méconnaissent l'article 34 de la Constitution, devaient être déclarées contraires à la Constitution (§. 78).

On observera que le Conseil constitutionnel n'a pas fondé sa décision sur une atteinte portée aux droits et libertés, mais sur le fait que le législateur n'avait pas épuisé sa compétence.

4. L'obligation de préciser et de compléter le dispositif envisagé par une loi spécifique relative aux mesures de surveillance des communications électroniques internationales

La loi relative au renseignement a donc été publiée le 24 juillet 2015 sans ces dispositions, créant ainsi un vide juridique qu'il importait de combler aussi rapidement que possible. C'est pourquoi des propositions de loi ont été déposées dès le mois de septembre, l'une à l'Assemblée nationale à l'initiative Mme Patricia Adam et M. Philippe Nauche, députés², l'autre au Sénat par M. Philippe Bas³, le Gouvernement ayant décidé d'inscrire celle déposée à l'Assemblée nationale le jour de l'ouverture de la session ordinaire et engagé sur ce texte la procédure d'examen accélérée.

Parallèlement à l'examen de cette proposition de loi à l'Assemblée nationale, le Président du Sénat, M. Gérard Larcher a, par lettre en date du 22 septembre 2015, saisi le Conseil d'État d'une demande d'avis sur la proposition de loi n° 700 déposée au Sénat par M. Philippe Bas⁴, très proche

¹ Décision n° 2015-713 DC du 23 juillet 2015 : <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html>

² Assemblée nationale - Proposition de loi n°3042 de Mme Patricia Adam et M. Philippe Nauche, déposée le 9 septembre 2015

³ Sénat- Proposition de loi n°700 déposée par M. Philippe Bas déposée le 21 septembre 2015.

⁴ Si le Conseil d'État est automatiquement saisi pour avis des projets de loi avant leur adoption en Conseil des ministres en application de l'article 39 alinéa 2 de la Constitution, cette saisine n'est pas obligatoire pour les propositions de loi. Le cinquième alinéa de l'article 39 donne néanmoins cette faculté au président d'une assemblée avant son examen en commission pour une proposition de loi déposée par l'un des membres de cette assemblée, sauf si ce dernier s'y oppose.

dans sa rédaction de celle examinée à l'Assemblée nationale ce qui a permis de conforter la sécurité juridique du texte.

Dans son avis rendu en assemblée générale le 15 octobre 2015, le Conseil d'État observe en premier lieu que « de nombreuses garanties, qui devaient initialement figurer dans un décret en Conseil d'État, sont désormais déterminées dans la loi elle-même » et que celle-ci répond « ce faisant, aux exigences qui découlent de la décision du conseil constitutionnel du 23 juillet 2015, et en particulier, de son § 78 en ce qui concerne la compétence du Parlement ».

Il estime que les différences substantielles instituées par le texte par rapport au régime de surveillance des communications nationales sont « justifiées à la fois par la différence de situation entre les personnes résidant sur le territoire français et celles résidant à l'étranger, par la différence corrélatrice des techniques de surveillance qui doivent être employées, ainsi que par la nature propre des missions de surveillance qui sont exercées à l'étranger ». Il observe d'ailleurs que « ce régime assortit la surveillance internationale de nombreuses conditions et garanties » et considère, dans ces conditions, que « la proposition de loi assure, sur le plan constitutionnel, une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, les nécessités propres aux objectifs poursuivis, notamment celui de la protection de la sécurité nationale, et d'autre part, le respect de la vie privée et le secret des correspondances protégés par les articles 2 et 4 de la déclaration des droits de l'homme et du citoyen ». L'ensemble de ces garanties permettent, selon le Conseil d'État, de « regarder l'ingérence dans la vie privée que rendent possible les mesures contenues dans la proposition de loi comme étant nécessaire, dans une société démocratique, à la sécurité nationale et à la prévention des infractions pénales, au sens de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».

Le Conseil d'État estime en troisième lieu que le régime de surveillance « ne méconnaît pas non plus des exigences constitutionnelles ou conventionnelles en ce qu'il ouvre la possibilité de surveiller pour les seules finalités prévues à l'article L.811-3 les personnes situées en dehors du territoire français (hormis le cas où elles utilisent des numéros d'abonnement ou des identifiants techniques rattachables au territoire national) sans prévoir de règles différentes selon leur nationalité ».

Il constate enfin que la proposition de loi, même si elle exclut le recours direct au juge contre les mesures prises au titre de l'article L.854-1, par les dispositifs qu'elle instaure, « ne méconnaît pas non plus le droit à un recours effectif reconnu par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».

En bref, le Conseil d'État n'a relevé d'incompatibilité entre le texte de la proposition de loi, ni avec les exigences posées par la jurisprudence du Conseil constitutionnel, ni avec celles posées par la jurisprudence de la Cour européenne des droits de l'Homme.

Dès lors, le Parlement a pu adopter un texte qui constitue le régime légal de la surveillance des communications électroniques internationales

dont le Conseil constitutionnel a établi la conformité à la Constitution par une décision n° 2015-722 DC du 26 novembre 2015¹.

5. Le nouveau cadre légal de la surveillance des communications électroniques internationales

L'article L. 854-1 du code de la sécurité intérieure indique d'abord, que la surveillance ne peut être autorisée qu'« *aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnées à l'article L. 811-3* » (voir supra)². Elle porte sur les « *communications qui sont émises ou reçues à l'étranger* ».

- Il précise ensuite, que les communications électroniques objets de la surveillance sont des données qui permettent un accès au contenu³ et des données de connexion.

- Il explicite l'articulation entre le régime applicable aux mesures de surveillance internationale et celui qui s'applique aux mesures de recueil de renseignement régies par la loi du 24 juillet 2015 relative au renseignement. Il est expressément indiqué qu'en principe, les mesures de surveillance internationale « *ne peuvent avoir pour objet d'assurer la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national* ». Les dispositions de l'article L. 854-1 s'articulent, par ailleurs, avec celles de l'article L. 854-8, propres aux communications dites « *mixtes* » auxquelles s'applique un régime particulier.

- À cette règle de principe, le législateur a cependant apporté une dérogation. La règle s'applique « *à l'exception du cas où ces personnes communiquent depuis l'étranger et, soit faisaient l'objet d'une autorisation d'interception de sécurité, délivrée en application de l'article L. 852-1, à la date à laquelle elles ont quitté le territoire national, soit sont identifiées comme présentant*

¹ Le Conseil constitutionnel en a déduit que l'ensemble des dispositions examinées « *ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* » (cons. 15). Il a également pris soin d'indiquer « *que le législateur a précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectés ainsi que celles du contrôle exercé par la commission nationale de contrôle des techniques de renseignement* » (cons.15). Cf. Conseil constitutionnel décision n° 2015-722 DC du 26 novembre 2015 <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-722-dc/decision-n-2015-722-dc-du-26-novembre-2015.146546.html>

² Ainsi, indique le Conseil constitutionnel, « *le législateur a précisément circonscrit les finalités permettant de recourir au régime d'autorisation des mesures de surveillance des communications émises ou reçues à l'étranger prévu par l'article L. 854-1 et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative* » (cons. 11).

³ Le texte utilisant le terme de « correspondances »

une menace au regard des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ».

- Lorsqu'elles sont captées, les communications entre personnes utilisant des numéros d'abonnement ou des identifiants rattachables au territoire national sont « *instantanément détruites* ».

L'article L. 854-2 décrit le régime des autorisations de surveillance des communications internationales. Ce régime comporte trois niveaux d'autorisation afin de le proportionner aux atteintes qu'elles sont susceptibles de porter au droit au respect de la vie privée.

- Il prévoit ainsi que le Premier ministre « *désigne, par une décision motivée, les réseaux de communications électroniques sur lesquels il autorise l'interception des communications émises ou reçues à l'étranger, dans les limites fixées à l'article L. 854-1* ». Les interventions techniques sont réalisées juridiquement par le Groupement interministériel de contrôle, organe placé sous l'autorité du Premier ministre.

- Ils distinguent ensuite les autorisations d'« *exploitation non individualisée des données de connexion interceptées* » des autorisations d'« *exploitation de communications, ou de seules données de connexion, interceptées* ». Dans les deux cas, les autorisations sont délivrées par le Premier ministre ou un de ses délégués à la demande des ministres de la défense, de l'intérieur, de l'économie, du budget ou des douanes ou de leurs délégués.

Dans le premier cas, l'autorisation désigne les finalités, les motifs et les services en charge de l'exploitation. Elle mentionne également « *le type de traitements automatisés pouvant être mis en œuvre, en précisant leur objet* ». L'autorisation est valable pour une durée d'un an, renouvelable selon la même procédure que pour l'autorisation initiale. Il s'agit d'une exploitation non ciblée des métadonnées qui permet aux services, notamment dans le domaine de la prévention du terrorisme de détecter des signaux faibles de menaces en exploitant des données non nominatives, de mettre en place des sélecteurs de recherche ou de détecter par exemple l'origine de cyberattaques...

Dans le second cas dont on déduit, par *a contrario*, qu'il s'agit de l'exploitation de communications « *individualisées* ». L'autorisation qui permet « *l'exploitation de communications, ou des seules données de connexion* » doit également délimiter les finalités poursuivies, les services en charge de l'exploitation et les motifs des mesures. Il incombe, en outre au Premier ministre ou à l'une des personnes qu'il délègue de désigner « *les zones géographiques ou les organisations, groupes de personnes ou personnes concernés* ». L'autorisation ne peut être donnée que pour une durée de 4 mois. Son renouvellement est décidé dans les mêmes conditions.

Parce que la loi a pour but de consolider la base juridique de la surveillance internationale et qu'elle crée des droits nouveaux, la prudence inciterait à définir de façon précise les modalités de mise en œuvre des procédures définies par le législateur. La DPR souhaiterait que les

autorisations en vigueur se voient doter d'un cadre plus formel. Cela consoliderait leurs bases juridiques, fournirait un cadre plus rigoureux pour les services et les ministres présentant des demandes d'autorisation, pour le Premier ministre et ses délégués, qui devront les instruire et les délivrer et l'intérêt, et pour la CNCTR, qui aux termes de l'article L. 854-9 en reçoit communication afin de pouvoir opérer son contrôle.

La DPR recommande au Premier ministre de définir dans les meilleurs délais, par le moyen d'une instruction générale, le cadre formel de présentation des demandes d'autorisation dans le respect des exigences posées par le législateur (*Proposition n°18*).

L'article L. 854-4 indique que l'interception et l'exploitation des communications font l'objet de dispositifs de traçabilité organisés par le Premier ministre après avis de la CNCTR et que le Premier ministre définit les modalités de centralisation des renseignements collectés.

La CNCTR a mis en place, en liaison avec la direction technique de la DGSE, les modalités du contrôle a posteriori. Un premier contrôle est déjà intervenu sur la base des méthodes précédemment définies. Un bilan sera établi dans les six prochains mois afin d'améliorer les outils techniques de ce contrôle.

L'article L. 854-5 définit les durées de conservation des données. Les durées de conservation des données sont, dans l'ensemble, supérieures à celles déterminées par la loi du 24 juillet 2015 et à celles établies pour les communications dites « *mixtes* » (art. L. 854-8).

Il prévoit notamment que :

- les correspondances sont conservées douze mois à compter de leur première exploitation, dans la limite de quatre ans après leur recueil ;
- les données de connexion sont conservées six ans après leur recueil ;
- la durée de conservation des renseignements chiffrés court à compter de leur déchiffrement mais dans la limite de huit ans après le recueil ;
- est applicable le régime de la conservation illimitée à des fins d'analyse technique en matière de cryptanalyse ou de cyberdéfense.

On peut, par ailleurs, noter que le Conseil constitutionnel a pris soin de relever que, comme dans le régime issu de la loi du 24 juillet 2015, les transcriptions ou extractions sont détruites dès que leur conservation n'est plus indispensable.

L'article L. 854-9 définit le contrôle qui s'exerce sur la surveillance des communications internationales.

Il énumère l'ensemble des prérogatives de la CNCTR reprenant celles prévues par l'article L. 833-2 du code de la sécurité intérieure issu de la loi du 24 juillet 2015, à l'exclusion de celles qui prévoient que la commission exerce d'un contrôle *a priori* sur les autorisations. On peut en particulier relever qu'est prévu son « accès permanent, complet et direct » aux dispositifs de traçabilité, aux transcriptions et extractions et aux renseignements collectés.

Le dispositif fait intervenir successivement le contrôle administratif de la CNCTR, puis le contrôle juridictionnel du Conseil d'État statuant dans des conditions permettant le respect du secret de la défense nationale. La commission peut s'autosaisir ou être saisie par toute personne qui pense être surveillée. S'agissant des mesures de surveillance des communications internationales, seule la CNCTR peut saisir le Conseil d'État. Comme dans le régime issu de la loi du 23 juillet 2015, cette saisine peut être pratiquée par le président de la commission ou par au moins trois de ses membres¹.

Le législateur a donc mis en place un cadre législatif, validé par le Conseil constitutionnel, conforme au droit constitutionnel interne. Sa conformité au droit européen, notamment à la CESDH reste à éprouver. Néanmoins, dans son avis sur la proposition de loi de M. Philippe Bas le Conseil d'État a mis en évidence sa compatibilité (voir supra)².

6. Hors territoire national

Par ailleurs, des techniques de renseignements sont susceptibles d'être utilisées à l'étranger ou dans des espaces communs. A priori, elles sont soumises soit au droit de l'État dans lequel elles sont utilisées et relèvent d'accords négociés, soit aux règles du droit international lorsqu'elles existent, s'agissant des espaces communs.

Il est probable qu'avec le développement des législations protectrices des droits de l'Homme et de la vie privée, un certain nombre d'États, mêmes partenaires seront, tôt ou tard, conduits à mettre en place un

¹ *Le Conseil constitutionnel a jugé* « que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure ; qu'en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale ; que les dispositions des quatrième et cinquième alinéas de l'article L. 854-9 doivent être déclarées conformes à la Constitution » (cons. 18). *Il admet ainsi, compte tenu de la nature des mesures de surveillance en matière de communications internationales et des modalités organisées pour permettre à la CNCTR comme au Conseil d'État d'exercer leur contrôle, que le recours susceptible d'être formé à l'encontre de mesures de surveillance internationale, qui présente un caractère intermédiaire, ne porte pas atteinte aux principes constitutionnels.*

² Conseil d'État, avis du 15 octobre 2015 (considérant 4) : <http://www.senat.fr/rap/l15-097/l15-0977.html#toc34>

cadre légal qui ne permettra d'agir qu'à travers des mécanismes de coopération et d'échanges, en limitant l'autonomie d'action de nos services.

Lors d'interventions militaires extérieures, les armées ont toute latitude pour intervenir ***.

B. LES COMMUNICATIONS ÉLECTRONIQUES INTERNATIONALES PAR VOIES HERTZIENNES

L'ancien article L. 241-3, créé par l'article 20 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications disposait que les transmissions empruntant la voie hertzienne ne sont soumises à aucune autorisation préalable du Premier ministre ni à aucun contrôle *a posteriori* par la CNCIS.

Dans son vingtième rapport d'activité, la CNCIS a rappelé que les dispositions de l'article L. 241-3 sont « *parfaitement distinctes des interceptions de sécurité et des procédures de recueil de données techniques de communications entrant dans le champ du contrôle de la CNCIS*¹. Elle a précisé que « *l'article L. 241-3 est relatif aux mesures générales de surveillance des ondes incombant au gouvernement pour la seule défense des intérêts nationaux et ne peut servir de base à la mise en œuvre d'interceptions de communications individualisables et portant sur une menace identifiée* ».

Cette surveillance est effectuée pour assurer la « *défense d'intérêts nationaux* » qui est une notion très large comme l'a rappelé la CNCIS : « *il appert que cette notion « d'intérêts nationaux » est très large et générique, incluant l'ensemble des « intérêts » de la communauté nationale, quel que soit le domaine considéré* »² Pour faire l'objet de cette surveillance, les transmissions concernées doivent emprunter la voie hertzienne et les mesures de surveillance et de contrôle doivent s'effectuer « *de manière aléatoire et non individualisée* ».

Ces mesures sont plus larges que les seules interceptions de sécurité ou le recueil de données techniques. Elles sont aussi par nature **aléatoires** et **non ciblées** sur une communication. Elles relèvent davantage d'une logique de prévention.

Au regard des évolutions technologiques, s'est rapidement posée la question des téléphones portables, dont les communications passent par la voie hertzienne. Dès 1998, la CNCIS a toutefois précisé que **le principe de liberté publique primait sur l'évolution technologique**, l'exception de l'article L. 241-3 devant ainsi s'interpréter strictement. La CNCIS rappelait ainsi dans son rapport pour l'année 1998 que « *toute interception de correspondance échangée par la voie des télécommunications, qui n'entre pas dans le*

¹ CNCIS, 20^{ème} rapport d'activité 2011-2012, pp. 40 et suiv.

² *Ibid.*, p. 43.

champ de l'article 20, est soumise quel que soit le mode de transmission filaire ou hertzien aux conditions et aux procédures fixées par la loi du 10 juillet 1991 ».

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement n'a pas modifié la rédaction issue de la loi de 1991, elle l'a simplement déplacée dans le code de la sécurité intérieure en créant un article L. 811-5 ainsi rédigé : *« Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent livre, ni à celles de la sous-section 2 de la section 3 du chapitre 1er du titre III du livre 1er du code de procédure pénale. »*

Dans son avis du 15 octobre 2015 précité, le Conseil d'État a conforté ce dispositif s'agissant de la surveillance des communications internationales que *« la référence au II de l'article L.854-1, au terme de « réseaux de communications électroniques n'a ni pour effet de modifier le champ d'application des mesures de surveillance tel qu'il a été défini par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement » et en précisant que « les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne continuent en effet, en application de l'ensemble du livre VIII du code de la sécurité intérieure, comme c'était déjà le cas dans la législation applicable antérieurement. »*

Le choix de retenir les numéros et les identifiants rattachables au territoire national plus que la nationalité des interlocuteurs offre également une sécurité juridique et une clarification pratique.

S'il offre aujourd'hui une protection juridique suffisante, le concept d'exception hertzienne, si utile et justifié soit-il, n'en demande pas moins une attention vigilante.

D'ores et déjà, il a subi quelques altérations :

- l'interprétation donnée par la CNCIS en 1998 dans son rapport d'activité (*voir supra*)
- l'insertion, dans les procédures d'autorisation et de contrôle, du recueil de renseignement au moyen de dispositifs de proximité ***.

Sans doute, l'interprétation de la CNCIS de 1998, devra-t-elle être confirmée par la CNCTR à la lumière de la nouvelle législation. Dans l'hypothèse d'une confirmation, il lui faudra, le cas échéant, décider, probablement par analogie, selon la nature des communications ou la localisation des points d'émissions et de réceptions du régime applicable (régime de communication nationale ou régime des communications internationales).

Dans la mesure où ces captations seraient réalisées à partir du territoire national, il est légitime de s'interroger sur la capacité des services à réaliser sur les ondes hertziennes des interceptions qui concerneraient des communications rattachables au territoire national, du moins à en exploiter

et à en conserver les données, si ces interceptions ne permettent pas d'identifier a priori les communications interceptées (sauf les dérogations du type de celle introduite à l'article L.854-1 du code de la sécurité intérieure s'agissant des communications électroniques internationales) ou les modalités selon lesquelles pourraient être exploitées des communications mixtes.

Il conviendrait également de s'interroger sur ce que recouvre la notion de territoire national, et sur son caractère attractif en droit international aux navires sous pavillon, aux aéronefs voire aux satellites.

Enfin, cette problématique pourrait être transposée à l'ingénierie de l'observation depuis l'espace aérien et l'espace extra-atmosphérique. Le développement de législations ou de jurisprudences protectrices de la vie privée et des droits de l'Homme applicables à la vidéosurveillance ou à l'usage des drones de loisir, y compris dans les espaces publics ou ouverts au public, notamment sur le territoire national pourrait à terme, par assimilation partielle et progressive, restreindre les capacités d'utilisation de ces outils.

Il est donc important que le Gouvernement, et notamment le SGDSN, en liaison avec les services juridiques des services spécialisés, soit attentif aux évolutions de tout un ensemble de législations concernant l'usage des technologies de la communication et de l'observation, mais aussi aux interrogations légitimes des citoyens, afin de trouver les modalités juridiques permettant d'apporter les réponses légales conciliant le besoin opérationnel des services et le respect des droits et de la vie privée comme la législation relative au renseignement a pu le faire en 2015.

IV. LA SURVEILLANCE INTERNATIONALE À L'ÉPREUVE DU TERRORISME

Aujourd'hui les moyens de la surveillance internationale sont utilisés face à la menace principale que constitue le terrorisme et notamment le groupe Daech, qui a organisé et revendiqué de nombreux attentats, en particulier ceux du 13 novembre. Néanmoins, dans la mouvance terroriste, d'autres ennemis ont manifesté la volonté d'organiser des actions sur le territoire national, comme Al-Qaida dans la Péninsule Arabique (qui a revendiqué l'attentat contre Charlie hebdo le 7 janvier, l'un des auteurs ayant séjourné au Yémen), ou contre nos intérêts ou nos forces armées qui les combattent comme Al-Qaida Maghreb Islamique et Al-Mourabitoune dans la bande sahélo-saharienne, Boko Haram..., enfin parmi les milices et rebellions hostiles qui menacent des pays amis, ***

A. UNE FORME NOUVELLE DE MENACE : FURTIVE, CHANGEANTE, ÉVOLUTIVE

Dans le contexte des attentats terroristes, nombre d'auditions réalisées par la délégation ont abordé l'état de cette menace. Celle-ci a fortement évolué et constitue une forme de rupture avec les mouvements observés jusqu'ici, même si certains protagonistes ont été impliqués par le passé dans des affaires liées au terrorisme, ce qui oblige les services spécialisés à une adaptation permanente.

1. Il s'agit d'une menace hybride.

Elle s'est enracinée dans des territoires en proie à des guerres civiles et qui ne sont plus contrôlés par des États souverains. Outre son expérience longue dans les activités terroristes et insurrectionnelles, le groupe Daech s'est agrégé notamment, en Irak, à des militaires professionnels et des cadres administratifs qui lui ont apporté la capacité de conquérir un territoire, d'y instaurer un proto-État où il assure les fonctions régaliennes, d'exploiter des ressources et d'attirer de nombreux combattants étrangers qu'il forme et utilise tant dans des actions militaires que dans des actions terroristes, les deux formes pouvant d'ailleurs se combiner. 40 % des 28 000 à 30 000 combattants de Daech sont aujourd'hui des étrangers et ce flux ne s'est pas ralenti.

2. Il s'agit d'une menace autoreproductrice

Elle a tendance à essaimer et à susciter des allégeances. Outre, les alliances d'opportunité de certaines tribus ou mouvements dans les zones d'activités de Daech, nombre de mouvements liés l'islamisme radical ont fait allégeance à ce groupe (comme Boko Haram au Nigeria). Il peut s'appuyer sur des dissensions au sein de groupes existants de la mouvance Al-Qaida, par exemple ou les Shebab en Somalie, porté par les succès engrangés en 2014 et au printemps 2015 en Irak et en Syrie. La situation de concurrence introduit un risque de surenchère entre ces groupes dans l'action terroriste à portée symbolique.

Toute situation d'instabilité ou de guerre civile larvée est exploitée dans le monde arabo-musulman pour infiltrer, installer, développer, contrôler des territoires. Ainsi en Libye, Daech a-t-il pu prospérer en contrôlant un territoire important autour de Syrte qui fait peser une menace sur la fragile Tunisie et plus au sud, potentiellement sur notre dispositif de sécurité de la bande sahélo-saharienne.

3. Il s'agit d'une menace matérielle et immatérielle

Ces groupes se sont dotés, comme jamais auparavant, d'un appareil de propagande moderne, utilisant les techniques les plus avancées de la communication, notamment les réseaux sociaux, la vidéo, l'Internet, pour convertir à leur cause de nombreux étrangers dans le monde entier, mais particulièrement dans le monde francophone et russophone¹.

Une partie de l'action militaire et terroriste s'est déplacée dans l'espace Internet (messageries, réseaux sociaux, *black forum...*). Les belligérants utilisent de plus en plus l'espace virtuel pour coordonner leurs actions et communiquer avec leurs partenaires.

4. Il s'agit d'une menace furtive

Ces groupes ont montré leur capacité à se mouvoir, dans un espace marqué par la liberté de circulation et de communication, malgré les mesures de surveillance mises en œuvre, montrant d'une certaine façon leurs insuffisances.

Même si elle est localisable, la menace terroriste, par sa furtivité, sa mobilité, son insertion dans la population, par son agilité dans l'utilisation des technologies modernes de communication et de télécommunication, et parce que le monde et le territoire européen sont plus ouverts à la circulation, s'affranchit des caractéristiques du milieu terrestre. Dès lors, le combat livré s'apparente davantage à ceux qui se jouent dans les espaces communs, où la liberté de mouvement est grande et l'offensive avantagée.

5. Il s'agit d'une menace capable de mener des actions terroristes dans le monde entier

Lorsqu'ils en ont les moyens, ces groupes peuvent mener des actions de type militaire, ce qui justifie l'action armée extérieure pour les réduire ; mais ils sont aussi capables, depuis leurs bases ou les régions où ils ont essaimé, de mener des actions terroristes. Un continuum est désormais clairement établi entre les théâtres extérieurs et le territoire national.

6. Il s'agit d'une menace de forte intensité

Ces groupes ont montré qu'ils étaient capables de mener des actions terroristes à long rayon d'action jusqu'à notre territoire national, grâce à des combattants aguerris et déterminés, prêts au sacrifice final ; grâce à des relais

¹ *Daech utilise Internet et y diffuse sa propagande par le biais de vidéo et de publications périodiques dont la délégation a pu consulter certains exemplaires.*

logistiques reposant sur des réseaux de solidarité parfois informels¹ mais opérant pour préparer leurs actions, loger leurs équipes, les doter en armement, en moyens de transports et de communication.

Il ne peut être totalement exclu que les techniques terroristes employées sur les théâtres du Levant ou du Sahel fassent leur apparition en Europe y compris sur le territoire national : utilisation de véhicules piégés, d'engins explosifs improvisés, de *snipers*...

Compte tenu des caractéristiques exposées, il s'agit d'une menace de forte intensité, résiliente et durable.

B. UN IMPACT SUR L'ORGANISATION DE LA SURVEILLANCE INTERNATIONALE

1. L'indispensable coopération interservices

La séparation administrative entre la sécurité extérieure et la sécurité intérieure est mise sous tension par la continuité de la menace portée par les flux de candidats au djihad en Syrie, le retour de combattants pour commettre des actes terroristes, le développement d'une propagande à fin de recrutement et l'utilisation de nouvelles techniques de communication, une certaine synthèse avec des formes de délinquance et de criminalité qui se distinguent des grands réseaux traditionnels de la criminalité organisée...

Dès lors, l'efficacité de l'action des services repose sur leur capacité à partager l'information acquise par leurs propres capteurs avec les autres services et souvent sur la fluidité de ces échanges.

Cette prise de conscience a conduit à revoir le fonctionnement interservices en France afin de disposer du meilleur renseignement au bon moment, à la fois, en incitant les services à un travail commun dans le recueil de l'information et surtout en facilitant le travail en commun dans l'exploitation des renseignements collectés.

La loi relative au renseignement permet le partage de toutes les informations entre les services utiles à l'exercice de leur mission.

Il convient de distinguer les accès aux capteurs et aux données ainsi que la nature de la coopération bilatérale ou multilatérale.

¹ Ces actions sont d'autant plus dangereuses qu'elles peuvent s'appuyer sur des combattants issus des pays visés, connaissant les lieux et les pratiques locales de surveillance, parfois issus de la délinquance, pouvant bénéficier de complicités parmi leurs proches, ou parmi ceux qui aspirent à les rejoindre.

a) La coopération dans l'emploi des capteurs

En fonction des sujets d'intérêt commun, il est fréquent que l'optimisation de l'emploi des capteurs soit recherchée afin d'éviter les doublons :

- soit en répartissant les missions de recueil entre les services associés dans le temps et dans l'espace ; à cet égard, il est important que les services qui sont opérateurs de certaines plateformes soient à l'écoute des besoins des autres services et que soit assuré, au niveau du Coordonnateur national du renseignement, un véritable travail de définition des priorités lorsque cela s'avère nécessaire ;
- soit en réalisant des missions communes ***.

b) La mise en place de cellule inter-agences

Pour les fournitures de données dans un cadre multilatéral ou bilatéral, l'environnement le plus propice est la mise en place de cellules interagences, ce qui suppose une volonté commune et la mise en place de systèmes d'information et de connexion opérationnels.

Il s'agit à ce stade de structures partenariales adaptées au besoin, créées de façon pragmatique et sans formalisme administratif particulier à l'exemple de la cellule Hermès mise en place pour renforcer le renseignement d'intérêt militaire en appui aux opérations militaires au Levant qui regroupe tous les services du premier cercle. Le croisement du renseignement permet d'appuyer les opérations militaires, mais aussi de protéger le territoire national face aux combattants étrangers de retour en Europe.

Compte tenu de la nature de la menace, la mise en place de façon pragmatique du travail collaboratif entre les services est utile et restera indispensable tant pour déjouer ou entraver les actions terroristes sur le territoire national que pour affaiblir les capacités de Daech au plus loin.

La DPR s'interroge néanmoins sur la place du CNR dans le suivi et l'évaluation du fonctionnement de ces dispositifs.

Elle souhaite, que cette coopération soit plus approfondie et que l'accès aux informations soit mieux partagé entre les services et que certaines procédures soient fluidifiées. (Proposition n°19)

On soulignera également tout le profit que la mobilité des personnels entre les différents services spécialisés de renseignement apporte dans les relations entre les services par une meilleure connaissance des moyens, des procédures et des personnes. Cet aspect a été souligné de façon récurrente par les deux directeurs généraux - DGSE et DGSIS - lors de leurs auditions par la délégation.

On soulignera également la complexité de l'action de renseignement de terrain sur un théâtre comme le Levant en raison de la concomitance de plusieurs types d'actions. Il faut en effet, tout à la fois, repérer et neutraliser, afin d'assurer la sécurité intérieure, les centres de décision susceptibles de commanditer des attentats terroristes ***, et identifier les réseaux familiaux ou tribaux susceptibles de réoccuper le terrain perdu par Daech et de constituer des forces vives pour apporter une solution à la crise syrienne et à l'équilibre nécessaire à une paix durable en Irak.

2. La complexe problématique européenne

L'Union européenne a perçu l'importance de la menace terroriste pour la stabilité des pays membres et la sécurité de leurs ressortissants.

Elle a développé ses compétences dans le domaine « justice et sécurité » ce qui est nécessaire dans un espace de libre circulation des personnes et des biens, mais dans une optique de protection maximale de ses principes plus que dans une réponse aux menaces, la compétence répressive restant entre les mains des États-membres.

a) L'institution d'un coordonnateur pour la lutte contre le terrorisme

L'Union européenne s'est donc très tôt orientée vers une démarche collaborative et facilitatrice, avec par exemple l'institution d'un coordonnateur européen pour la lutte contre le terrorisme.

Cette institution est probablement utile dans un certain nombre de domaines prospectifs, mais elle est faible, sauf peut-être pour les pays ne disposant pas de capacités fortes dans ce domaine du renseignement opérationnel. Cependant n'ayant pas de capacités opérationnelles à offrir, il est à craindre que cette instance puisse être dépassée par la coopération directe entre les services des grands États qui ont des informations à échanger et des capacités à mettre en œuvre.

La difficulté à organiser une coopération entre les services de renseignement, autrement que par des accords bilatéraux, est patente. Elle est également rendue complexe par l'hétérogénéité des modes d'organisation des services et des législations en vigueur dans les différents États membres. Sans doute, « n'est-il pas nécessaire d'espérer pour entreprendre ni de réussir pour persévérer ». Tout effort qui pourra conduire à l'établissement de relations plus denses entre les différents services de renseignement européen et à suivre le parcours de personnes soupçonnées de vouloir commettre des attentats terroristes dans l'un ou l'autre des pays membres de l'Union européenne constituera une avancée et l'amorce d'une pratique.

b) La sous-utilisation du Système d'information Schengen (SIS)

Il est malheureusement paradoxal de constater après la survenance d'un attentat que l'on parvient à retracer le parcours de tel ou tel auteur, à travers les enquêtes de police, et à relever les lacunes dans la transmission des informations qui, si elle avait pu intervenir à temps, aurait probablement permis d'entraver l'action. Autant, la coopération paraît possible a posteriori sur le fondement de la pratique de la police judiciaire (Europol et Interpol) autant paraît-elle plus difficile dans le domaine préventif du renseignement.

Face à l'évolution de la menace terroriste (*voir supra p. 73*), à la mobilité des acteurs concernés et à leur nombre, il est impératif d'optimiser l'efficacité des outils automatisés permettant leur suivi. Les fiches de surveillance diffusées à travers le réseau SIS constituent un outil à la disposition des services de renseignement. On ne peut que déplorer que la DGSI soit la seule à alimenter régulièrement ce fichier et le caractère très lacunaire des informations fournies par les services des autres pays membres de l'Union européenne.

Une révision ciblée du code frontière Schengen permettrait d'harmoniser et d'encadrer les pratiques tout en garantissant leur pérennité.

Le Conseil européen du 12 février 2015 s'est prononcé en ce sens, sans pour autant recueillir l'unanimité parmi les États-membres et au sein de la Commission.

Le code Schengen n'interdit pas les contrôles électroniques systématiques des titres à l'entrée dans l'espace Schengen pour les ressortissants européens afin de vérifier si leurs documents ne sont pas volés, falsifiés ou invalidés. Mais le code interdit l'accès systématique au SIS pour vérifier les informations de police et de justice relatives aux personnes contrôlées. Une évolution sur ce point est nécessaire. La Commission devait déposer fin 2015 ou début 2016 une proposition relative au « paquet frontières intelligentes » intégrant une révision du code.

Il est probable que la crise des réfugiés de 2015 constituera un incitatif puissant à renforcer les contrôles aux frontières extérieures de l'espace Schengen. Il reste que l'inertie propre au système de décision européen, la nécessaire mise en œuvre par chacun des États-membres et la réalisation de systèmes d'information nécessaires demanderont du temps. C'est pourquoi, il convient d'agir avec célérité et en attendant de conforter les relations bilatérales entre services.

La prise de conscience des gouvernements européens à la suite des attentats terroristes survenus en 2015 permettra d'avancer en ce domaine. La DPR encourage le Gouvernement français à saisir toutes les opportunités pour y parvenir, lui demande d'inciter ses partenaires à mieux renseigner le fichier SIS, renouvelle sa recommandation concernant l'amélioration du code frontière Schengen notamment son article 7 et formule le souhait que le renforcement de l'efficacité des contrôles aux frontières extérieures de l'espace Schengen soit examiné par les instances européennes au premier trimestre 2016 (*Proposition n°20*)

Les conclusions de la réunion des Chefs d'État et de gouvernement le 18 décembre 2015 à Bruxelles vont dans ce sens en convenant d'introduire systématiquement dans le système Schengen de deuxième génération (SIS II) les données sur les combattants terroristes étrangers et le partage des données concernant les personnes en lien avec le terrorisme et le crime organisé et l'extension du système ECRIS aux nationaux de pays tiers.

c) Le laborieux aboutissement du PNR

La délégation avait déploré le trop grand retard pris par le projet au sein des instances européennes, notamment au Parlement européen, et recommandé dans son rapport pour 2014 de mettre en place le système PNR à l'échelon national dans les plus brefs délais.

Un accord visant à surmonter les dernières divergences a été conclu le 4 décembre 2015 entre les États-membres de l'Union européenne. Cet accord est susceptible de dénouer ce blocage observé depuis cinq ans. Il vise à répondre aux objections du Parlement européen en limitant à 6 mois la durée de rétention, pendant laquelle les États peuvent conserver les données transmises par les transporteurs aériens sans en masquer les aspects les plus sensibles (la France demandait un an). Il contient également l'engagement de tous les États pour que tous les vols intra-européens et les vols charters soient inclus. Cette position commune a été approuvée par la commission des libertés civiles du Parlement européen le 10 décembre. Le projet de directive devrait être soumis en séance plénière au début de l'année 2016, adopté par le conseil des ministres et transposé dans les législations des États-membres.

Il reste cependant en deçà des besoins exprimés par les services de renseignement.

Si le projet de directive prévoit le transfert par les transporteurs aériens vers des « unités de renseignement sur les passagers » des États-membres, des données PNR des passagers de vols extra-UE¹, il n'obligera pas les États-membres à appliquer ces dispositions aux vols intra-UE. Cette

¹ A savoir à partir d'un pays tiers vers un État-membre de l'UE et vice-versa

extension est autorisée, elle procèdera d'un acte volontaire des États qui devront en informer la Commission par un avis écrit.

De même les agences et organisateurs de voyage qui fournissent des services tels que les réservations de vols, pour lesquels ils recueillent et traitent les données PNR, ne sont pas inclus dans le champ d'application de la directive. Les États-membres sont autorisés à prévoir, conformément à leur droit national, un système de collecte et de traitement des données détenues par ces opérateurs.

Les données PNR ne peuvent être traitées que pour la prévention et la détection d'infractions terroristes et d'infractions graves, ainsi que la réalisation d'enquêtes et de poursuites en la matière. La liste unique des infractions a été établie, incluant notamment, la traite des êtres humains, la participation à une organisation criminelle, la cybercriminalité, la pédopornographie ainsi que le trafic d'armes, de munitions et d'explosifs.

Les données PNR fournies par les transporteurs aériens aux unités nationales de renseignement sur les passagers devraient être conservées pendant une période de cinq ans. Pendant les six premiers mois, elles pourront inclure les données d'identification personnelle, au-delà ces données devront être masquées¹. Le conseil cherchait à prolonger la période au cours de laquelle les données sont entièrement accessibles à deux ans (contre 30 jours dans la proposition initiale de la Commission en 2011).

Les députés ont introduit des garanties de protections des données (conditions d'accès, supervision, contrôle interne).

Enfin, il est prévu une clause de révision deux ans après sa transposition en droit national. La nécessité d'introduire des opérateurs économiques autres que les transporteurs aériens dans le cadre de la directive devrait être examinée au cours de ce processus de révision.

Elle prend également note de l'entrée en phase de production de SETRADER, avec un spectre limité à vingt compagnies aériennes pour des vols en partance ou en provenance de dix pays⁽²⁾.

Il lui paraît souhaitable d'accélérer la montée en charge du système SETRADER, en lien avec le déploiement du PNR. (Proposition n°21)

¹ Dépersonnaliser les données en les masquant signifie rendre certains éléments de ces données invisibles pour un utilisateur, par exemple le(s) nom(s) – notamment les noms d'autres passagers mentionnés dans le PNR et le nombre de passagers voyageant ensemble figurant dans le PNR – l'adresse, les coordonnées, etc (à savoir les éléments qui pourraient servir à identifier directement le passager auquel les données PNR font référence.

(2) Les pays concernés sont : l'Algérie, l'Égypte, le Liban, le Mali, le Maroc, la Mauritanie, le Niger, le Tchad, la Tunisie et la Turquie.

S'agissant du système national, si la DPR peut se réjouir de l'achèvement du cadre juridique nécessaire au développement et à l'exploitation d'un tel système, notamment avec le complément apporté par la loi n° 2015-917 du 28 juillet 2015 portant actualisation de la loi de programmation militaire et la publication du décret n° 2015-1328 portant modification de l'article 5 du décret n° 2010-569 du 28 mai 2010 qui permet désormais le criblage du fichier des personnes recherchées avec le système API-PNR en France, elle déplore que des difficultés techniques aient conduit à différer la livraison du système d'information à une date non déterminée courant 2016. Une préfiguration de la plateforme d'exploitation du système, l'Unité information passagers (UIP) a ouvert les locaux aménagés à Roissy en septembre.

La DPR recommande que la transposition de la directive PNR puisse être examinée par le Parlement français dans les trois mois suivant son adoption et que puisse être mis en œuvre sans délai le projet de PNR national (Proposition n°22)

d) Une avancée en matière de système spatial d'observation

Si sur le plan militaire, l'idée d'une défense européenne tarde à émerger, il convient de se réjouir des accords conclus en 2015 avec l'Allemagne pour la réalisation du programme du système spatial d'observation MUSIS et la lettre d'intention signé par la France, l'Allemagne, l'Italie et l'Espagne en matière de recherche pour une nouvelle génération de drones MALE.

3. La coopération internationale entre services

Compte tenu de l'internationalisation de ses champs d'action, de la décentralisation potentielle de ses centres de décisions, mais aussi de la facilité croissante des communications dans le monde, et notamment en Europe, l'efficacité de la lutte contre le terrorisme, repose pour une part croissante sur la capacité à identifier et à suivre les protagonistes dans leurs déplacements et dans leurs échanges, et donc sur la coopération et les échanges avec des services de renseignement étrangers.

« *La lutte contre le terrorisme est un terrain, par excellence, de confiance et de mutualisation avec nos partenaires, et le succès de nos opérations est fonction de notre capacité à échanger* »¹, selon le Coordonnateur national du renseignement.

¹ Didier Le Bret intervention lors de la 13^{ème} Université d'été de la défense - Strasbourg 15 septembre 2015

Si la plupart des États condamnent vigoureusement le terrorisme et affichent des résolutions de principe pour le combattre en facilitant la coopération, les échanges entre les services devraient se trouver facilités. Sur le plan opérationnel, tel n'est pas toujours le cas, soit parce que derrière les intentions, la hiérarchie des objectifs stratégiques ne coïncide pas entièrement, soit parce que la culture interne de la coopération et de l'échange n'est pas développée, soit parce que certains pays ne disposent pas de capacités suffisantes.

La coopération et les échanges sont faciles lorsqu'il s'agit d'un dialogue entre puissances de premier rang, ils demeurent complexes dans les autres cas.

Lors de leurs auditions, les services ont souligné les progrès réalisés dans les échanges avec ***.

4. La concentration des efforts ne doit pas se faire au détriment des autres missions qui demeurent stratégiques

La concentration des efforts sur la lutte contre le terrorisme si indispensable soit-elle, ne doit pas conduire nos services à renoncer à leurs autres missions dans le domaine de la contre-ingérence, du renseignement économique, de la contre-prolifération et de la lutte contre la criminalité organisée. Ce serait sacrifier des années d'effort et nous mettre en péril à l'avenir.

<p>La montée en puissance des services de renseignement a pu être réalisée par l'affectation de moyens supplémentaires et non par redéploiement interne ce qui aurait pu être le choix en période de tension budgétaire. La DPR souhaite que le Gouvernement puisse maintenir cet effort dans la durée (<i>Proposition n°23</i>).</p>
--

5. Une problématique qui dépasse la seule action des services de renseignement et la seule réponse militaire

L'évolution de la menace dans sa forme comme dans son intensité a suscité une réponse cohérente et proportionnée par le renforcement des moyens affectés à la sécurité nationale et à la défense dont les services de renseignement, par leur action préventive, constituent un élément déterminant.

Elle a conduit également à la mise en œuvre de procédures exceptionnelles sur le territoire national comme le recours aux forces armées en appui aux forces de police, pour assurer la sécurité (adaptation en cours du plan Vigipirate, opération Sentinelle). Le recours à l'Armée dans ses missions de protection fera l'objet d'un rapport du SGDSN dont le Parlement

sera saisi au début de l'année 2016. **La DPR se montrera attentive à la façon dont les moyens de renseignement militaire pourront être, le cas échéant, mis en œuvre dans le cadre de ces dispositifs.**

Elle a conduit au Levant à une action militaire en deux temps avec l'opération Chammal en Irak, puis avec l'intervention en Syrie, pour combattre Daech, la force constituant en ces circonstances le seul moyen d'arrêter la violence.

Pour autant, certains aspects du phénomène sont inédits par leur masse et leur caractère exponentiel comme celui de la radicalisation extrême de jeunes, y compris dans des pays démocratiques. Ces phénomènes nouveaux demandent des réponses appropriées. La surveillance renforcée sur le territoire national, comme à l'international ne constitue qu'un élément de la réponse. Il ne saurait être le seul comme l'ont souligné les travaux parlementaires consacrés à la lutte anti-terroriste publiés cette année à l'Assemblée nationale et au Sénat.

La surveillance doit conduire à l'action préventive ou répressive. Elle doit aussi permettre d'analyser plus finement les causes profondes et permettre l'élaboration de mesures préventives très en amont, mais qui ne relèvent pas du domaine des services de renseignement.

Les premiers pas ont été effectués pour lutter contre la propagande et le recrutement, avec des systèmes de signalement, des centres de « déradicalisation » et des outils de contre-propagande sur l'Internet (mis au point notamment par le service d'information du gouvernement), mais ces moyens restent encore expérimentaux. Il reste de vastes champs d'étude et d'action pour comprendre les causes profondes et les ressorts de ces phénomènes afin de leur apporter des réponses appropriées qui relèvent probablement davantage des domaines social et culturel que du ressort strictement sécuritaire.

La DPR souhaitait mentionner cette nouvelle dimension, non pour dédouaner les services de renseignement qui n'ont peut-être pas su détecter suffisamment tôt les signaux faibles de ce phénomène sous-jacent, ni, lorsqu'ils en ont perçu l'importance et les risques, être suffisamment écoutés par les autorités politiques, mais pour souligner qu'elle constitue une rupture et doit être traitée dans toutes ses dimensions, ce qui implique une réponse politique globale.

V. LES PROPOSITIONS DE LA DPR

10/ Organiser des retours d'expériences réguliers sur les dispositifs collaboratifs et coopératifs mis en place par les services, pour en améliorer le fonctionnement et à terme servir de base à une réflexion sur une éventuelle réorganisation. L'organisation du recueil de ces retours d'expériences pourrait être confiée au CNR en s'appuyant au besoin sur la définition d'une méthodologie d'évaluation préparée par l'inspection des services de renseignement.

11/ Procéder à ***

12/ Procéder à ***

13/ Mettre en place un dispositif d'évaluation *** et inclure ces indicateurs dans le rapport d'activité des services qui est transmis chaque année à la DPR.

14/ Demander au CNR de s'assurer, *** et qu'au besoin, il soit en mesure de réaliser les arbitrages nécessaires.

15/ S'assurer de ***

16/ Demander au CNR ***.

17/ Amplifier les efforts entrepris pour conforter les moyens du renseignement humain.

18/ Définir dans les meilleurs délais par le moyen d'une instruction générale du Premier ministre, le cadre formel de présentation des demandes d'autorisation dans le respect des exigences posées par le législateur dans la loi du 27 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

19/ Compte tenu de la nature de la menace, la mise en place de façon pragmatique d'un travail collaboratif entre les services est indispensable tant pour déjouer ou entraver les actions terroristes sur le territoire national que pour affaiblir les capacités de Daech au plus loin.

Définir la place du CNR dans le suivi et l'évaluation du fonctionnement des dispositifs de travail collaboratif entre les services, notamment dans le cadre de la lutte contre le terrorisme.

Approfondir cette coopération pour améliorer l'accès aux informations et fluidifier certaines procédures.

20/ Saisir toutes les opportunités pour faire progresser la coopération européenne dans le cadre de la lutte contre le terrorisme, inciter nos partenaires et les instances européennes à mieux renseigner le fichier SIS, à améliorer le code frontière Schengen notamment son article 7 et à examiner le renforcement de l'efficacité des contrôles aux frontières extérieures de l'espace Schengen au premier trimestre 2016.

21/ Accélérer la montée en charge du système SETRADER, en lien avec le déploiement du PNR.

22/ Inscrire à l'ordre du jour du Parlement, le projet de loi de transposition de la directive PNR dans les trois mois suivant son adoption et mettre en œuvre sans délai le projet de PNR national.

23/ Poursuivre dans la durée l'effort de montée en puissance des services de renseignement par l'affectation de moyens supplémentaires et non par redéploiement interne.

CHAPITRE IV L'ÉVALUATION DE LA POLITIQUE PUBLIQUE DE RENSEIGNEMENT

L'évaluation de la politique publique de renseignement fait partie, depuis la loi de programmation militaire (LPM) pour les années 2014 à 2019¹, des missions de la délégation parlementaire au renseignement (DPR).

Jusqu'alors cantonnée au « *suivi de l'activité générale et les moyens des services spécialisés* », il s'agissait pour elle d'une « *mutation philosophique importante* »² dont elle s'est saisie rapidement. Son rapport d'activité pour l'année 2014, qui comprenait notamment des développements importants consacrés au renseignement économique et financier (REF), aux ressources humaines et à la réforme du renseignement intérieur, et formulait 103 propositions, en constitue le premier témoignage.

Le vote de la loi du 24 juillet 2015 relative au renseignement³, qui attribue des moyens nouveaux aux services de renseignement, et les attentats qui ont frappé la France durant l'année 2015 appellent naturellement de la part de la délégation la plus grande vigilance dans l'exercice de cette mission, nouvelle pour elle.

Il importe pour cela que les dispositions législatives qui prévoient la communication à la DPR de différents éléments d'information soient à présent pleinement mises en œuvre. Seule une information parfaitement documentée, avec des indicateurs dans la mesure du possible standardisés, transmise de façon régulière, pourra permettre à la délégation de constituer des séries et effectuer des comparaisons pertinentes d'un exercice à l'autre.

I. LES APPORTS DE LA LOI DU 24 JUILLET 2015 RELATIVE AU RENSEIGNEMENT

Avec la loi du 24 juillet 2015 relative au renseignement, la France s'est enfin dotée d'un cadre juridique clair et unifié en matière de renseignement et a fait sortir de l'ombre une politique publique qui émerge véritablement depuis quelques années seulement. Elle a, pour la première fois, donné une définition à la politique publique de renseignement et renforcé sensiblement les moyens d'information de la DPR.

¹ Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

² Rapport d'activité 2014 de la délégation parlementaire au renseignement, par M. Jean-Jacques Urvoas, député, 18 décembre 2014, p. 13.

³ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

A. LA DÉFINITION D'UNE POLITIQUE PUBLIQUE DU RENSEIGNEMENT

Si la LPM 2014-219 avait consacré, pour la première fois au niveau législatif, la notion de politique publique de renseignement, elle n'en avait pas donné de contenu.

Sa mention à l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires n'était en effet destinée qu'à permettre à la délégation parlementaire au renseignement d'exercer son rôle, nouveau pour elle, de contrôle de l'action du Gouvernement et d'évaluation de la politique publique dans ce domaine.

C'est donc la loi du 24 juillet 2015 qui a donné un contenu à cette politique publique de renseignement.

Le nouvel article L. 811-1 du code de la sécurité intérieure, issu d'un amendement du rapporteur au nom de la commission de la défense, M. Philippe Nauche, dispose ainsi que « *la politique publique de renseignement concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation* ». Cet article fait référence à deux notions bien définies par ailleurs par le législateur : celle de « *stratégie de sécurité nationale* », définie à l'article L. 1111-1 du code de la défense et celle de « *d'intérêts fondamentaux de la Nation* », définie à l'article 410-1 du code pénal.

Article L. 1111-1 du code de la défense (extraits) : « La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter. »

Article 410-1 du code pénal : « Les intérêts fondamentaux de la Nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel. »

À l'initiative de M. Pascal Popelin, il a été précisé, dans ce même article L. 811-1 que cette politique publique relevait « *de la compétence exclusive de l'État*. » Il s'agissait alors de souligner que cette politique ne « *saurait faire l'objet ni d'une sous-traitance à des sociétés privées ni d'une privatisation* »¹.

¹ Rapport n° 2697 au nom de la commission des lois sur le projet de loi relatif au renseignement, par M. Jean-Jacques Urvoas, député, 2 avril 2015, p. 99.

Le nouvel article L. 811-2 du même code de la sécurité intérieure définit pour sa part les missions assignées aux services spécialisés de renseignement. Ceux-ci ont ainsi pour missions « *en France et à l'étranger, la recherche, la collecte, l'exploitation et à la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces. Ils agissent dans le respect de la loi, sous l'autorité du Gouvernement et conformément aux orientations déterminées par le Conseil national du renseignement.* »

Jusqu'ici éparpillées dans les différents décrets constitutifs de ces administrations, les missions des services de renseignement sont donc, là aussi pour la première fois, définies par le législateur.

Grâce aux précisions de la loi du 24 juillet 2015, la politique publique du renseignement dispose donc désormais d'un contenu et les services spécialisés d'une mission fixée par le législateur.

B. LES MOYENS D'INFORMATION DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT COMPLÉTÉS

Les moyens d'information de la délégation parlementaire au renseignement avaient été élargis une première fois par rapport au texte initial de 2007¹ par la LPM 2014-2019 pour lui permettre d'exercer au mieux sa mission nouvelle de contrôle et d'évaluation.

1. Les documents communiqués à la DPR

Le I de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 disposait ainsi que devaient être communiqués à la DPR les documents suivants :

« 1° *la stratégie nationale du renseignement* » : il s'agit d'un document public qui fixe, pour un horizon de cinq ans, les grands axes de la politique du Gouvernement en matière de renseignement. Ce document a été transmis à la DPR en octobre 2014 et a fait l'objet d'une publication sur le site Internet de l'Académie du renseignement ;

« 2° *des éléments d'informations issus du plan national d'orientation du renseignement* » (PNOR). Le PNOR est la déclinaison annuelle de la stratégie nationale, à destination des services. Il s'agit donc d'un document à vocation opérationnelle, couvert par le secret de la défense nationale. La première version de ce PNOR avait été présentée à la délégation le 27 novembre 2014 par le Coordonnateur national du renseignement ;

¹ Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

« 3° un rapport annuel de synthèse exhaustif des crédits consacrés au renseignement et le rapport annuel d'activité des services spécialisés de renseignement ». Deux rapports de synthèse des crédits ont été transmis à la DPR à ce jour, en septembre 2014 pour l'exercice 2013 et en septembre 2015 pour l'exercice 2014. Le rapport annuel d'activité n'a pas été jusqu'à présent transmis à la délégation mais devrait l'être pour la première fois en 2016 sur l'exercice 2015.

« 4° des éléments d'appréciation relatifs à l'activité générale et à l'organisation des services spécialisés de renseignement ». Tout au long de l'année, la DPR a demandé et reçu un certain nombre de documents de la part des services pour préparer son rapport d'activité.

La loi du 24 juillet 2015 a complété cette liste des documents à transmettre à la DPR, à la suite de plusieurs amendements de M. Jean-Pierre Raffarin, président de la commission des affaires étrangères et de la défense du Sénat.

Les services de renseignement du « second cercle », c'est-à-dire n'appartenant pas à la communauté du renseignement, ont ainsi été intégrés dans le champ de contrôle de la DPR. Les 3° et 4° de l'article 6 *nonies* disposent désormais que le rapport annuel de synthèse des crédits et les éléments sur l'activité générale des services porteront également sur les « services autorisés par le décret en Conseil d'État mentionnée à l'article L. 811-4 » du code de la sécurité intérieure à recourir aux techniques de renseignement prévues par la loi. Ils précisent également que ces informations ne concerneront que les activités de renseignement de ces services.

Cela élargit considérablement le champ d'action de la DPR puisque le décret en Conseil d'État publié le 11 décembre 2015¹ établit une liste très complète des services autorisés à recourir à ces techniques. Y sont ainsi notamment mentionnées, au sein de la police nationale, la direction centrale de la police judiciaire, la direction centrale de la police aux frontières, la direction centrale de la sécurité publique ; au sein de la gendarmerie nationale, la sous-direction de l'anticipation opérationnelle et les sections de recherche ; la sous-direction du renseignement territorial ; les sections de recherche de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement (*voir supra Chapitre II et Annexe 6*)

Par ailleurs, toujours à l'initiative du président Jean-Pierre Raffarin, la loi du 24 juillet 2015 a ajouté un 5° à l'article 6 *nonies* de l'ordonnance pour prévoir une transmission à la DPR des « observations que la Commission nationale de contrôle des techniques de renseignement adresse au Premier ministre [...] ainsi qu'une présentation, par technique et par finalité, des éléments

¹ Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure.

statistiques » figurant dans son rapport d'activité. Si de nombreuses informations sont déjà comprises dans le rapport public de cette commission, le Gouvernement n'avait pas souhaité que la présentation par technique et par finalité soit rendue publique. Il était en revanche légitime que la DPR soit destinataire de ce type d'informations.

L'article 21 de la loi relative au renseignement a également pris en compte, d'une part, la possibilité pour la délégation de saisir la CNCTR (article L. 833-11 du code de la sécurité intérieure) et, d'autre part, la transmission des observations que la CNCTR adresse au Premier ministre (article L. 833-10).

2. Une extension de la liste des personnes susceptibles d'être entendues par la DPR

Enfin, la liste des personnes pouvant être entendues par la délégation, déjà enrichie par la LPM 2014-2019¹, a été complétée par la loi du 24 juillet 2015 à l'initiative de M. Jean-Jacques Urvoas, président de la commission des lois de l'Assemblée nationale, contre l'avis du ministre de l'Intérieur². Peuvent désormais être auditionnés, outre les directeurs des services spécialisés de renseignement, éventuellement accompagnés des collaborateurs de leurs choix « *toute personne placée auprès de ces directeurs et occupant un emploi pourvu en conseil des ministres* ». Il s'agit d'ailleurs de la mise en œuvre d'une proposition formulée par la délégation parlementaire au renseignement dans son rapport d'activité 2014.

Cette disposition permettra de recevoir les cadres de ces services, sans que le ministre ou le directeur du service ne puissent s'y opposer. Un nombre assez large de personnes est en réalité concerné : les officiers généraux occupant des fonctions de sous-directeurs au sein de certains services de renseignement et les emplois « à la décision du Gouvernement » traditionnellement prévus en conseil des ministres.

Ceci intègre naturellement les directeurs des services du « second cercle ». La DPR a ainsi procédé à l'audition, le 3 septembre dernier, des

¹ La délégation peut aujourd'hui entendre le Premier ministre, les ministres compétents, le secrétaire général de la défense et de la sécurité nationale, le directeur de l'Académie du renseignement, les directeurs des services spécialisés, les directeurs d'administration centrale ayant à connaître l'action des services, le président de la Commission nationale de contrôle des techniques de renseignement et le président de la Commission consultative du secret de la défense nationale.

² Lors de l'examen au Sénat du projet de loi relative à la programmation militaire (LPM) pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (Loi n° 2013-1168 du 18 décembre 2013), la question de la délimitation du champ des personnes pouvant être auditionnées par la délégation avait déjà fait l'objet de débats. Notre collègue Jean-Pierre Sueur avait proposé que la délégation puisse entendre, avec l'accord des directeurs de service et en leur présence, tous les agents des services. Toutefois, le Gouvernement avait sous-amendé cette disposition en ne prévoyant que la possibilité pour les directeurs des services de se faire accompagner des collaborateurs de leur choix.

responsables de la sous-direction à l'anticipation opérationnelle (SDAO) de la Gendarmerie nationale, de la DRPP et du SCRT

La loi du 24 juillet 2015 a également prévu la possibilité pour la délégation parlementaire au renseignement d'entendre chaque semestre le Premier ministre sur son application ainsi que les personnes spécialement déléguées par lui pour délivrer les autorisations de mise en œuvre des techniques de renseignement mentionnées par la loi.

Celle-ci peut également inviter le président de la CNCTR à lui présenter le rapport d'activité de la commission, tout comme le président de la Commission consultative du secret de la défense nationale.

II. UNE MISE EN ŒUVRE ENCORE TIMIDE

S'il n'est naturellement pas possible de dresser un premier bilan de la mise en œuvre des dispositions votées à l'été 2015, on peut commencer à effectuer un premier retour d'expérience de celles qui étaient présentes dans la LPM 2014-2019.

A. LA STRATÉGIE NATIONALE DU RENSEIGNEMENT ET LE PLAN NATIONAL D'ORIENTATION DU RENSEIGNEMENT

La stratégie nationale du renseignement a été communiquée à la délégation parlementaire au renseignement en octobre 2014 et est depuis consultable sur le site Internet de l'Académie du renseignement¹.

Elle définit la politique du renseignement pour les cinq ans à venir et est publiée « *pour mieux faire connaître à nos concitoyens le rôle essentiel que jouent les services dédiés à cette mission, dans la défense et la promotion de nos intérêts fondamentaux* » peut-on y lire.

Cinq menaces majeures y sont identifiées :

- le terrorisme, « *menace permanente, évolutive et diffuse* » : « *les services de renseignement sont chargés de détecter les individus ou groupes à risques et d'empêcher le passage à l'acte* » ;

- l'espionnage, « *atteinte à notre souveraineté et à notre indépendance* » : « *les services exercent une surveillance constante de ces activités d'espionnage et les entravent lorsqu'elles sont détectées [...] L'enjeu est la sauvegarde de notre indépendance scientifique, technologique et économique et la préservation de l'emploi* » ;

- « *la prolifération des armes de destruction massive, une menace permanente contre la paix* » : il s'agit là de la « *collecte d'informations à travers le monde* » ainsi que le suivi des « *flux d'armement à travers le monde* » ;

¹ www.academie-renseignement.gouv.fr

- « le cyber, un espace anonyme et ouvert propice à toutes les agressions » : « les services de renseignement se mobilisent afin d'être en mesure d'identifier les agresseurs existants ou potentiels, d'évaluer leurs capacités et leurs intentions à court, moyen et long terme » ;

- « la criminalité internationale, un fléau qui menace la cohésion des États » : « les services contribuent à la surveillance et au démantèlement de ces réseaux criminels [...] La surveillance des routes de la drogue et des réseaux criminels mafieux très structurés originaires d'Europe centrale et du Caucase constitue une priorité ».

La stratégie nationale rappelle enfin que « le renseignement extérieur est un instrument de promotion et de défense des intérêts de la France dans le monde ». Elle rappelle notamment que « les zones de crise ou celles dans lesquelles la France a des intérêts stratégiques sont prioritaires » et qu'une « attention particulière est accordée à la protection de nos approvisionnements stratégiques en ressources et matières premières. »

Telle qu'elle est rédigée, la stratégie nationale du renseignement est donc une déclinaison, à destination des services de renseignement, des priorités fixées par le Livre blanc sur la défense et la sécurité nationale de 2013.

Le plan national d'orientation du renseignement (PNOR) est un document opérationnel destiné aux services de renseignement auxquels il fixe la feuille de route. Présenté pour la première fois à la DPR le 27 novembre 2014, il comporte un certain nombre de rubriques et définit des priorités pour les services en fonction de l'analyse de l'état de la menace.

Ce document n'est naturellement pas public et la DPR n'en n'est pas destinataire mais est seulement informée de certains de ses éléments, afin qu'elle n'ait pas à connaître d'éléments opérationnels, ce qui entrerait en contradiction avec la jurisprudence du Conseil constitutionnel sur ce point¹.

C'est néanmoins ce document qui a vocation à servir de référence pour l'évaluation de la politique de renseignement conduite par le Gouvernement et qui servira donc de support au futur rapport d'activité des services de renseignement (*Voir infra.*)

B. LE RAPPORT ANNUEL DE SYNTHÈSE DES CRÉDITS CONSACRÉS AU RENSEIGNEMENT

Pour la deuxième année consécutive, la délégation parlementaire au renseignement a reçu le rapport annuel de synthèse des crédits consacrés au renseignement. La présentation des crédits y est déclinée par ministère et par service, en reprenant la nomenclature des différents programmes

¹ Décision n° 2001-456 DC du 27 décembre 2001.

budgétaires qui concourent à leur financement. Les montants en fonds spéciaux alloués à chacun des services y figurent également.

Ce rapport a été établi sur le même périmètre que le précédent : il comprend les six services qui composent la communauté du renseignement ainsi que certaines administrations qui concourent à la fonction « renseignement » :

- la direction générale de l'armement et l'état-major des armées, pour ce qui concerne les études amont et les achats de matériels spécifiques ;
- le secrétariat général de la défense et de la sécurité nationale, pour les investissements interministériels ;
- le haut fonctionnaire de défense et de sécurité des ministères économiques et financiers, qui finance l'indemnisation des opérateurs de télécommunications électroniques au titre des prescriptions qui leur sont imposées ;
- le groupement interministériel de contrôle ;
- la direction du renseignement de la préfecture de police de Paris ;
- l'Académie du renseignement ;
- la Coordination nationale du renseignement.

Pour l'exercice 2014, ce rapport indique que l'exécution des crédits de l'ensemble des administrations concourant à la fonction « renseignement » a été de *** euros, dont *** pour les six services de la communauté du renseignement.

À la fin de l'année 2014, *** ETPT¹ étaient mobilisées au titre de la fonction « renseignement », dont la grande majorité, ***, au sein de la communauté du renseignement, précise également le rapport.

Ce document, pour intéressant qu'il soit pour la délégation parlementaire au renseignement, appelle de sa part plusieurs remarques :

- **Son calendrier tout d'abord.** Il porte sur l'exécution de l'année N-1 et lui est transmis à l'automne de l'année N. Il aurait été intéressant, comme la DPR en avait fait la remarque dans son rapport d'activité 2014, qu'il comporte des éléments sur l'exécution de l'année en cours.

- **L'absence de présentation des crédits de l'année à venir, ensuite.** La DPR avait également fait cette observation l'année dernière, **il est regrettable que le document ne présente pas les crédits de l'année à venir, c'est-à-dire de l'année N + 1.** Le rapport de synthèse des crédits de l'année

¹ ETPT : équivalent temps plein travaillé.

2014 présente ainsi les crédits de l'année 2015 mais ne présente pas ceux prévus par le projet de loi de finances pour 2016. C'est d'autant plus dommage qu'au moment où ce document est transmis à la DPR, à l'automne, les arbitrages budgétaires gouvernementaux ont déjà été rendus et les crédits inscrits dans le projet de loi de finances de l'année à venir. Disposer d'éléments d'informations budgétaires consolidés aurait été intéressant pour les parlementaires de la délégation, appelés à se prononcer sur le projet de loi de finances au même moment.

***, il est envisagé d'accélérer les travaux de préparation du rapport annuel de synthèse des crédits afin qu'il ne soit plus remis à l'automne mais au printemps de l'année N + 1. Dans ce cas, on comprend aisément qu'il ne soit plus possible de présenter l'exécution des crédits de l'année en cours ou les crédits inscrits dans le projet de loi de finances pour l'année à venir. Une présentation plus précoce est cependant certainement plus pertinente.

<p>La DPR demande la remise du rapport annuel de synthèse des crédits au printemps de l'année N+1 (<i>Proposition n°24</i>)</p>
--

• **L'absence d'indicateurs, enfin.** On peut regretter que **le rapport ne comporte pas plus d'indicateurs.** Il comprend certes des commentaires, des indications sur l'évaluation des emplois que l'on ne trouve naturellement pas dans les documents budgétaires rendus publics chaque année par le Gouvernement mais aucun indicateur de performance, par exemple, n'y figure alors qu'ils sont présents dans les projets annuels de performance (PAP) et les rapports annuels de performance (RAP).

À ce jour, seuls deux services de la communauté du renseignement disposent d'indicateurs de performance liés à leurs activités, présentés chaque année dans les PAP et RAP : la direction du renseignement militaire (DRM) et la direction de la protection et de la sécurité de la défense (DPSD).

- Au sein du programme 144 « Environnement et prospective de la politique de défense » de la mission « Défense », l'objectif 2 s'intitule « Améliorer le niveau de sécurité des forces et du patrimoine industriel et économique lié à la défense » et concerne la DPSD.

L'indicateur 2.1 « *Taux d'avis dans les délais prescrits* » mesure ainsi la performance de la chaîne « habilitation » de la DPSD à travers les délais d'enquête nécessaires à la délivrance des habilitations aux différents personnels de la défense. L'indicateur 2.2 « *Taux des sites du domaine militaire et des sites industriels et économiques liés à la défense inspectés dans les délais prescrits* » mesure pour sa part les inspections conduites par la DPSD pour s'assurer que les sites sensibles sont maintenus au meilleur niveau de sécurité. Le catalogue des sites et la périodicité des inspections ne figurent naturellement pas dans le PAP mais pourraient être utilement communiqués à la DPR au cas où ces indicateurs seraient intégrés au rapport sur les crédits.

- Au sein du programme 178 « Préparation et emploi des forces » de la mission « Défense », l'objectif 1 a pour mission d'assurer la fonction stratégique connaissance-anticipation. L'indicateur 1.1 « *Taux de satisfaction de la fonction stratégique connaissance-anticipation* » concourt à cette mission. Il mesure notamment la capacité de la DRM à satisfaire ses commanditaires en termes de délais et de qualité.

Si l'on comprend que l'activité de tous les services ne se prête pas facilement à ce genre de chiffrages, et encore moins à leur publication, la délégation parlementaire au renseignement pourrait cependant être destinataire, dans le cadre du rapport de synthèse des crédits, d'éléments d'informations complémentaires qui lui permettraient d'apprécier plus précisément les indicateurs de performance aujourd'hui publiés.

L'élaboration du futur rapport d'activité des services de renseignement sera précisément l'occasion de réfléchir à la mise en œuvre d'une telle démarche de performance pour l'ensemble des services de renseignement.

La DPR demande que des indicateurs de performance figurent dans le rapport de synthèse des crédits (*Proposition n°25*).

C. LE RAPPORT ANNUEL D'ACTIVITÉ ET L'ORGANISATION DES SERVICES DE RENSEIGNEMENT

Si le premier rapport annuel de synthèse des crédits a été élaboré dès l'année qui a suivi le vote de la LPM, le premier rapport d'activité des services de renseignement n'a en revanche pas trouvé de concrétisation à ce jour. Parmi les six services qui composent aujourd'hui la communauté du renseignement, un seul publie chaque année un rapport d'activité complet, TRACFIN, tandis que les résultats obtenus par la DNRED sont agrégés dans le résultat de la direction générale des douanes et des droits indirects.

L'année 2015 a cependant été mise à profit par l'inspection des services de renseignement, saisie en ce sens par le cabinet du Premier ministre, pour réfléchir à ce que devraient être les contours de ce futur rapport d'activité¹.

¹ Établissement d'un rapport d'activité des services de la communauté du renseignement, rapport au Premier ministre – novembre 2015.

L'inspection des services de renseignement

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

Placée sous l'autorité directe du Premier ministre, elle 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* » selon l'article 2 du décret.

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...) 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, le mandat et la composition de l'équipe. Le secrétariat de l'inspection est assuré par la Coordination nationale du renseignement.

La DPR, en vertu 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. En 2015, deux lui ont été transmis : celui sur le rapport d'activité des services et un autre sur ***.

Dans son rapport d'activité 2014, la DPR proposait que l'inspection se dote d'un véritable chef, afin qu'il incarne « une certaine permanence en dépit de l'absence d'un corps d'inspection pérenne »¹. Cette disposition n'a malheureusement pas été mise en œuvre à ce jour mais elle ne semble pas exclue à l'avenir.

La délégation parlementaire au renseignement souhaiterait également que, sur le modèle de coopération instauré de longue date entre la Cour des comptes et le Parlement, elle puisse demander à l'inspection des services de renseignement de réaliser des études pour son compte. Il ne s'agirait naturellement de placer cette inspection sous sa tutelle mais de pouvoir simplement bénéficier d'une partie de son ordre du jour afin de compléter, sur des points précis, le travail accompli par la délégation.

La DPR réitère sa demande de nomination d'un chef de service à la tête de l'inspection des services de renseignement (*Proposition n°26*).

Elle souhaite pouvoir saisir l'inspection des services de renseignement de thèmes d'études (*Proposition n°27*).

Les membres de la délégation parlementaire au renseignement ont exprimé, au cours de leur réunion du 16 juillet 2015, leur point de vue sur le contenu de ce futur rapport et transmis, par l'intermédiaire de son président, M. Jean-Pierre Raffarin, leurs attentes à l'inspection des services.

¹ Rapport d'activité 2014, *op. cit.*, p. 72.

Aux yeux de la délégation, le rapport d'activité doit notamment comprendre :

« 1. Un rappel des objectifs fixés par la stratégie nationale du renseignement et par le plan national d'orientation du renseignement. Une présentation des objectifs nouveaux assignés aux services, par rapport à ces textes cadres, pour l'année concernée » ;

« 2. Une présentation de l'activité de chacun des services [...] qui s'efforcera de mettre en exergue les productions concrètes des services à partir d'outils statistiques (indicateurs d'activité) qui pourraient être issus de leurs tableaux de bord internes et en établissant des comparaisons avec les exercices antérieurs [...]. Elle pourra être illustrée par des cas concrets à l'image des cas typologiques présentés dans le rapport d'activité de TRACFIN » ;

« 3. Une présentation des moyens (budgétaires, humains, matériels) comprenant des éléments statistiques avec des comparaisons avec les exercices antérieurs [...]. Une présentation des politiques RH de recrutement, de déroulement de carrière et de formation des personnels [...]. Une présentation des politiques d'investissements (acquisition, recherche) » ;

« 4. Une présentation transversale de la coordination entre les services à travers une description des modes de coopération institués ou occasionnels et des éléments statistiques. »

« 5. Une présentation des activités de coopération internationale ».

Le président Jean-Pierre Raffarin précisait également dans le courrier adressé au chef de mission de l'inspection des services de renseignement que la forme du rapport devait être exhaustive et que les données et outils statistiques mis en place devaient « permettre la constitution de séries et comparaisons d'un exercice à l'autre ».

Là est en effet bien l'enjeu de ce futur rapport d'activité pour la DPR : disposer d'éléments chiffrés, standardisés d'un service à l'autre et comparables année après année pour évaluer la politique du Gouvernement dans le domaine du renseignement.

Au stade actuel de la réflexion, il pourrait être prévu une élaboration en plusieurs temps : chaque service élaborerait son propre rapport d'activité, qui serait ensuite transmis au Coordonnateur national du renseignement (CNR). Celui-ci élaborerait alors un document de synthèse qui serait ensuite transmis à la DPR, après relecture par les services et leurs ministres de tutelle et validation par le Conseil national du renseignement.

Les services de renseignement utiliseraient une trame pour l'élaboration de leurs rapports :

- une première partie serait consacrée à la synthèse de leur activité, en rappelant les principales évolutions intervenues dans l'année (menaces, missions, moyens humains et techniques, organisation, évolutions juridiques et technologiques), les forces et les faiblesses du service, l'adéquation des

moyens aux missions, l'état de la coordination avec le deuxième cercle de la communauté ainsi que le respect de la réglementation ;

- une deuxième partie serait plus spécifiquement dédiée à la mesure de la performance, aux résultats, aux activités et moyens au regard des différentes rubriques du PNOR. Chaque partie du PNOR serait ainsi associée à un indicateur de performance (nombre de notes diffusées sur la thématique concernée, nombre d'actions d'entraves, nombre d'interceptions autorisées, nombre de signalements...), ou si cela n'était pas possible, à un cas concret. Les services pourraient également s'attacher à préciser les suites ayant prolongé leur activité : nombre de judiciarisations, nombre d'actions de préventions. Il n'existe pas de difficulté particulière des services à présenter techniquement leur contribution aux priorités qui leur ont été dévolues, tous disposant ou ayant progressivement construit des tableaux de bord internes ou à destination de leur ministre permettant de suivre leur activité en lien avec les priorités du PNOR.

- les activités non couvertes par le PNOR, telles que les missions spécifiques, les échanges et rencontres avec les services étrangers ainsi que les actions de formation feraient enfin l'objet d'une partie spécifique.

Le rapport transmis à la DPR reprendrait les éléments de ces rapports d'activité auxquels le CNR ajouterait une appréciation sur l'état de la coordination entre les différents services ainsi qu'une synthèse générale.

Il est proposé que le rapport d'activité de l'année N soit transmis à la DPR au printemps (mars-avril) de l'année suivante. Il est proposé que le premier rapport porte sur l'année 2015, ce à quoi la délégation souscrit totalement.

<p>La DPR demande que le rapport annuel d'activité des services de renseignement lui soit présenté au cours du premier semestre de l'année N+1 (<i>Proposition n°28</i>).</p>
--

Il est envisagé également l'élaboration d'un document destiné à être rendu public, afin de mieux faire connaître l'activité des services de renseignement et renforcer la culture du renseignement en France, qui fait encore défaut. Les membres de la délégation parlementaire au renseignement¹, qui travaillent depuis plusieurs années à l'émergence de cette politique publique, ne peuvent que se féliciter de cette initiative, qui viendra compléter l'information qu'elle délivre elle-même chaque année dans ses rapports d'activité.

¹ Cf. par exemple, *Pour un « État secret » au service de notre démocratie*, rapport d'information n° 1022 de MM. Jean-Jacques Urvoas et Patrice Verchère au nom de la commission des lois de l'Assemblée nationale, 14 mai 2013.

La DPR demande l'élaboration et la diffusion d'un rapport public élaboré par le CNR, afin de mieux faire connaître l'activité des services de renseignement et de développer la culture du renseignement (*Proposition n°29*).

Tel qu'il est envisagé ***, le rapport d'activité semble donc correspondre aux attentes de la délégation parlementaire au renseignement. Il convient toutefois de souligner que depuis que l'inspection a été saisie, le vote de la loi du 24 juillet 2015 impose désormais que ce rapport d'activité traite également des services du « second cercle » qui mettent en œuvre les techniques de renseignement prévues par cette même loi, pour ce qui concerne leurs activités de renseignement.

La délimitation étendue du « second cercle », retenue par le décret du 11 décembre 2015, ne saurait justifier un nouveau retard dans la mise au point du rapport annuel d'activité des services de renseignement et sa communication à la DPR.

III. LES PROPOSITIONS DE LA DPR

24/ Remettre le rapport annuel de synthèse des crédits au printemps de l'année N+1

25/ Faire figurer des indicateurs de performance dans le rapport de synthèse des crédits

26/ Nommer un chef de service à la tête l'inspection des services de renseignement.

27/ Donner à la DPR la capacité de saisir l'inspection des services de renseignement de thèmes d'études

28/ Communiquer le rapport annuel d'activité des services de renseignement à la DPR au cours du premier semestre de l'année N+1.

29/ Elaborer et diffuser un rapport public élaboré par le CNR, afin de mieux faire connaître l'activité des services de renseignement et de développer la culture du renseignement.

CHAPITRE 5 : LE RAPPORT GÉNÉRAL DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX

PREMIER RAPPORT PUBLIC DE LA COMMISSION DE VÉRIFICATION DES FONDS SPÉCIAUX

*

* *

Composition de la CVFS pour l'année 2015

-Michel Boutant, sénateur

-François-Noël Buffet, sénateur

-Jacques Myard, député

-Jean-Jacques Urvoas, député, président de la CVFS

INTRODUCTION

La Commission de vérification des fonds spéciaux (CVFS) a été fondée en 2001 et transformée à l'occasion du vote de la loi de programmation militaire en décembre 2013. Depuis cette date, elle est une formation spécialisée de la délégation parlementaire au renseignement (DPR) et incarne l'organe de contrôle parlementaire de ces masses financières utilisées par les services de renseignement pour assumer leurs missions essentielles.

Depuis son premier exercice en 2002, la CVFS n'avait jamais publié de rapport public, la loi ne le prévoyant pas mais ne l'interdisant pas explicitement non plus. Le présent document constitue donc une première dont la survenance paraît nécessaire.

En effet, si le respect du secret de la défense nationale impose de ne pas communiquer des informations qui profiteraient *in fine* à nos adversaires, il n'empêche en rien d'aborder des questions d'intérêt public de manière publique. Comme cela avait pu être le cas pour le rapport de la DPR pour l'année 2014, nous estimons que le contrôle parlementaire s'exerce certes au profit du Parlement, mais avant tout à destination de nos concitoyens qui ont le droit et le besoin de connaître - pour reprendre une terminologie juridique fréquente en ce domaine - les actions conduites en leur nom ou, à tout le moins, les supports financiers de ces opérations.

Le présent rapport revient donc sur l'histoire du contrôle des fonds spéciaux et souligne les progrès accomplis en la matière. Il plaide d'ailleurs pour l'approfondissement de ceux-ci et formule plusieurs préconisations en ce sens. Il aborde certains aspects liés à la gestion et l'utilisation des fonds spéciaux et appelle à des évolutions au service d'une plus grande efficacité dans le strict respect des conditions légales.

Mais le secret ne se conjugue ni avec l'arbitraire ni avec l'impunité et l'architecture de contrôles patiemment bâtie depuis 2012 en témoigne : la rénovation de la DPR en décembre 2013, la création d'une inspection des services de renseignement en juillet 2014, l'institution de la Commission nationale de contrôle des techniques du renseignement (CNCTR) et d'une formation spécialisée du Conseil d'État en juillet 2015 témoignent de cette volonté ardente de soumettre à des contrôles complémentaires, techniques et systématiques les autorités politiques et les administrations que celles-ci dirigent. Or l'action de la CVFS s'inscrit pleinement dans ce cadre en ce qu'elle participe d'un contrôle externe et, par ses préconisations, aide à l'amélioration du contrôle interne.

Dans cet esprit, il convient également de préciser que ce rapport se complète de huit procès-verbaux protégés par le secret de la défense nationale en raison des informations qu'ils contiennent. Ces documents sont issus des missions de contrôle réalisées sur pièces et sur place ainsi que des auditions conduites au sein de la Direction générale de la sécurité extérieure (DGSE), de la Direction générale de la sécurité intérieure (DGSI), de la Direction du renseignement militaire (DRM), de la Direction de la protection et de la sécurité de la Défense (DPSD), de la Direction nationale du renseignement et des enquêtes douanières (DNRED), de Tracfin, du Groupement interministériel de contrôle (GIC), du cabinet du Premier ministre et de la Coordination nationale du renseignement.

Ces procès-verbaux formulent une centaine de recommandations qui portent tant sur la gestion des fonds spéciaux, le contrôle interne réalisé que les usages de ces masses financières ou les règles d'attribution.

Comme évoqué précédemment, l'objectif du rapport public mais également des procès-verbaux réside dans la mise en place d'une solide doctrine du contrôle parlementaire afin qu'elle fasse jurisprudence et complète l'édifice construit patiemment depuis 2012. De même, les recommandations souhaitent guider le perfectionnement des mécanismes de contrôle interne - au sein de l'exécutif comme des services de renseignement - au-delà des aspects comptables dans la mesure où les fonds spéciaux concernent plus généralement l'activité de ces services. Cette exigence est d'autant plus aiguë que le Gouvernement a consenti des moyens financiers et humains exceptionnels en même temps qu'il a restructuré la communauté du renseignement notamment au travers de la création de la DGSI, du Service central du renseignement territorial...

Plus que jamais, le renseignement est devenu une politique publique au service de notre sécurité et de notre modèle démocratique. Plus que jamais, nos concitoyens en ressentent l'impérieuse utilité au regard de la plurivocité des menaces qui parfois endeuillent notre pays. Or, comme toute politique publique, celle-ci est soumise au regard exigeant de nos concitoyens et de leurs représentants. Le présent rapport souhaite illustrer cet état de fait.

I. LE CONTRÔLE DES FONDS SPÉCIAUX OU LA LONGUE MARCHÉ DU PARLEMENTARISME

Longtemps considérés comme un élément constitutif de la souveraineté de l'État, voire de la raison d'État, les fonds spéciaux répondent en réalité à une nécessité opérationnelle et tactique des services de renseignement. En effet, ces derniers doivent pouvoir disposer de moyens financiers destinés à soutenir, dans les plus brefs délais et une parfaite confidentialité, des activités opérationnelles correspondant à leurs missions légales en application de la loi du 24 juillet 2015 et aux instructions des autorités gouvernementales.

De fait, leur utilisation et leur contrôle ne sauraient répondre aux règles traditionnelles de la comptabilité publique tant les informations fournies par des pièces comptables sont susceptibles de révéler la nature des missions conduites, les personnes qui y contribuent, les méthodes employées... Ces sommes ont donc été soustraites à deux règles majeures de la comptabilité publique : le principe de séparation des ordonnateurs et des comptables (dans le cas des fonds spéciaux, le service consommateur assure la gestion et le contrôle) ainsi que celui de spécialité budgétaire (le Parlement dans son intégralité vote uniquement une enveloppe sans connaître l'affectation précise ⁽¹⁾).

Or, cette spécificité justifie l'existence d'un contrôle particulier qui a échoué aux parlementaires jusqu'en 1852 et leur échoit à nouveau depuis 2001. Mais l'évolution n'est pas encore achevée et des modifications semblent aujourd'hui nécessaires pour le perfectionner.

A. QUAND L'ÉTAT SECRET EST AUSSI UN ÉTAT DE DROIT

1. Une tradition monarchique revivifiée mais rectifiée par la Quatrième République

Alors que le contrôle des fonds spéciaux constitue indubitablement une avancée pour l'État de droit, un examen historique rappelle que cette pratique s'avère fort ancienne. Elle apparaît en effet sous l'Ancien Régime, à l'époque de Louis XIII, mais subit de lourds dévoiements à tel point que, en 1789, près d'un quart des finances publiques françaises relevait abusivement des fonds secrets ⁽²⁾. Et en 1820, lorsque le budget du ministère de l'Intérieur intégra une rubrique « Dépenses spéciales pour les dépenses secrètes de la police » ⁽³⁾, une commission spéciale composée de deux parlementaires fut

(1) Comme le note David Biroste, in « Les fonds spéciaux : contribution à l'étude des marges du droit (première partie) », *Revue française de finances publiques*, décembre 2002, n°80, p. 154, « leur existence n'est pas secrète, leur destination seulement ».

(2) *Ibid.*

(3) *Ibid.*

instituée afin de contrôler ces masses financières. La Monarchie de Juillet perpétua d'ailleurs l'initiative. Toutefois, cette activité ne bénéficiait que d'une faible publicité à l'occasion de l'examen du budget, l'un des deux parlementaires se contentant de se présenter à la tribune et de déclarer sur l'honneur que l'usage des sommes allouées était convenable ⁽¹⁾.

Étonnamment, la République ne se conforma pas à cette coutume, déniait au pouvoir législatif ce que la monarchie lui avait accordé, en dépit de la volonté de certains parlementaires ⁽²⁾. Appelés fonds secrets ou fonds libres (notamment par Joseph Barthélémy dans son *Traité de droit constitutionnel*), ces dotations financières n'acquiescent une existence publique qu'au début de la Quatrième République, au détour de l'article 42 de la loi du 27 avril 1946 portant ouverture et annulation de crédits sur l'exercice 1946. N'étant alors plus secrets, ils prirent en conséquence le nom de « spéciaux » et leur gestion fut confiée au seul Président du Conseil ⁽³⁾. Cependant, le texte législatif n'envisageait aucun contrôle en dehors de l'établissement d'un décret de *quitus* mentionnant, pour chaque ministre, les sommes reçues, les sommes dépensées et le reliquat (lequel devait être annulé, comme tout crédit non consommé). Pour autant, ces dispositions n'ont jamais été appliquées ⁽⁴⁾. Quant au contrôle parlementaire, il était balayé au profit d'un simple rappel – rendu irréal par la nature même de l'objet – du principe de responsabilité du Gouvernement devant le Parlement qui se cantonnait au vote d'un montant global sans connaître ni l'affectation ni l'utilisation réelle. Dans les faits, au moment de la discussion de la loi de Finances, le Rapporteur spécial de chaque chambre était courtoisement informé par le Secrétaire général du Gouvernement – s'il en faisait la demande – de la ventilation des masses financières concernées, sans capacité inquisitoriale supplémentaire en raison du secret de la défense nationale.

Un an plus tard, rompant partiellement avec ce qui s'apparente à un blanc-seing législatif, le décret n° 47-2234 du 19 novembre 1947 instaura un contrôle interne des fonds utilisés par le seul SDECE (service de documentation extérieure et de contre-espionnage, l'ancêtre de la DGSE), contrôle exercé par une commission de vérification *ad hoc*. Les autres services de renseignement, les cabinets ministériels et certains ministères demeuraient hors de portée de tout contrôle ⁽⁵⁾.

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

(2) Comme le rappelle David Biroste, « Les fonds spéciaux... (première partie) », article cité, p. 181.

(3) Le premier alinéa de l'article 42 de la loi de 1946 limitait l'ouverture des crédits de fonds spéciaux au seul budget du chef de l'exécutif qui était chargé de mettre à la disposition des ministres les dotations nécessaires au fonctionnement de leurs départements respectifs.

(4) Comme l'établit le rapport rédigé par François Logerot, « Note à l'attention de Monsieur le Premier ministre relative au régime des fonds spéciaux », 10 octobre 2001, 20p.

(5) Sur l'affectation des fonds spéciaux à cette époque, se reporter à David Biroste, « Les fonds spéciaux... (première partie) », article cité.

Composée d'un Président de chambre à la Cour des comptes (président de la commission) et de deux commissaires nommés par décret du Président du Conseil parmi les membres du Conseil d'État, de la Cour des comptes ou de l'Inspection générale des finances, la structure était chargée de vérifier l'adéquation entre les sommes allouées, les dépenses effectuées et les pièces justificatives fournies par le SDECE (article 7 du décret). Cette tâche accomplie, elle devait remettre un rapport au Président du Conseil et au ministre des Finances, rapport ensuite transmis à la Cour des comptes, laquelle certifiait, dans sa déclaration générale de conformité, que le montant indiqué correspondait bien aux sommes décaissées.

Pour accomplir sa mission, la Commission était dotée de larges prérogatives dans la mesure où elle pouvait se faire présenter tous les documents nécessaires à sa démarche et même procéder à la vérification de l'état sommaire des dépenses des opérations en cours. Elle avait également la faculté de déléguer l'un de ses membres pour réaliser des enquêtes dans le but de contrôler les faits retracés dans les documents comptables présentés par le SDECE. Toutefois, ces capacités étaient mises en œuvre pour effectuer un contrôle uniquement comptable (régularité des ordres de paiement, pièces justificatives afférentes), sans prendre en considération la question de l'opportunité de l'utilisation de ces fonds. Ce périmètre correspondait parfaitement à la philosophie d'un contrôle interne.

2. La CVFS : un contrôle parlementaire né d'une polémique (2001)

L'instance fonctionna dans la plus parfaite discrétion jusqu'à sa disparition en 2001. Mais, comme évoqué, son champ de compétence ne concernait que le service de renseignement extérieur et ne venait en rien contrarier l'usage discrétionnaire des fonds spéciaux par les autres services de renseignement, le Premier ministre et l'exécutif en général. Aussi, le 4 juillet 2001, en pleine polémique sur l'utilisation des fonds spéciaux par le Président Jacques Chirac pour financer des déplacements personnels, le Premier ministre de cohabitation Lionel Jospin demanda à titre personnel au Premier président de la Cour des comptes François Logerot de lui adresser des propositions dans le cadre d'un réexamen d'ensemble du régime des fonds spéciaux. En parallèle, deux propositions de loi furent déposées à l'Assemblée nationale afin de mieux encadrer ces masses financières : la première était portée par Jean-Louis Debré ⁽¹⁾, la seconde par Philippe de Villiers ⁽²⁾. Si le député de Vendée n'évoquait aucun mécanisme de contrôle de l'utilisation des fonds spéciaux, l'ancien ministre de l'Intérieur préconisait en revanche la création d'une commission présidée par le Premier président

(1) Proposition de loi n° 3245 de MM. Jean-Louis Debré, Philippe Douste-Blazy et Jean-François Mattéi, relative à la transparence du fonctionnement des pouvoirs publics et portant suppression des fonds spéciaux, 16 juillet 2001.

(2) Proposition de loi n° 3238 de M. Philippe de Villiers, tendant à supprimer les fonds spéciaux tels que définis à l'article 42 de la loi n° 46-854 du 27 avril 1946, 16 juillet 2001.

de la Cour des comptes au sein de laquelle auraient siégé des parlementaires ainsi que des membres du Conseil d'État et des magistrats de la Cour de cassation. Cette commission devait procéder au contrôle de l'ensemble des fonds spéciaux désormais réservés aux seuls enjeux de sécurité.

Néanmoins, le projet de loi de finances pour 2002, déposé le 18 septembre 2001 par le Gouvernement, ne prévoyait nullement une réforme de ces fonds spéciaux. Ce ne fut qu'en octobre que deux amendements de l'exécutif vinrent proposer l'instauration de la Commission de vérification des fonds spéciaux (CVFS) après que François Logerot eut remis au Premier ministre son rapport ⁽¹⁾. Le document et les amendements défendaient une optique proche de celle des propositions de loi précitées.

En effet, le Premier président concluait à la nécessité de maintenir le régime dérogatoire des fonds spéciaux pour permettre à l'État de « *pouvoir conduire dans le secret l'action de protection de la sécurité intérieure et extérieure de la collectivité nationale* ». Il jugeait notamment « *légitime que soit conservée la ligne budgétaire réservée à la DGSE* » et demandait le maintien à son profit « *d'un compte de dépôts échappant aux contrôles habituels en matière de dépense publique* ». Il proposait également que cette ligne « *soit élargie aux autres services concourant à la recherche du renseignement* ». Il soulignait en revanche que toutes les dépenses n'ayant pas de rapport avec la protection de la sécurité intérieure et extérieure de l'État devaient être réintégrées dans les lignes budgétaires de droit commun destinées à financer des dépenses de rémunérations ou de fonctionnement.

François Logerot recommandait enfin le maintien d'un contrôle sur les fonds spéciaux de la DGSE afin « *de vérifier la sincérité des imputations dont ils font l'objet et d'en rendre compte au gouvernement* ». Selon lui, il convenait également de l'étendre à l'ensemble des services détenteurs de fonds spéciaux, mais aucune proposition n'était formulée quant à ses modalités concrètes.

Un consensus semblait donc se dégager autour de l'idée de restreindre l'usage de ces fonds aux seules questions de sécurité tandis que les parlementaires souhaitaient intégrer la structure chargée de leur contrôle (en conformité avec l'article 14 de la Déclaration des droits de l'Homme et du Citoyen : « *Tous les Citoyens ont le droit de constater, par eux-mêmes ou par leurs Représentants, la nécessité de la contribution publique, de la consentir librement, d'en suivre l'emploi et d'en déterminer la quotité, l'assiette, le recouvrement et la durée.* »)

Fort de ces préconisations consensuelles, le Gouvernement fit preuve d'une inventivité limitée lorsqu'il s'est agi de définir le périmètre de la

(1) Rapport consultable sur le site de la Documentation française : <http://www.ladocumentationfrancaise.fr/rapports-publics/014000737-note-a-l-attention-de-monsieur-le-premier-ministre-relative-au-regime-des-fonds>

nouvelle Commission de vérification des fonds spéciaux ⁽¹⁾ instituée à l'article 154 de la loi de finances pour 2002 : il se contenta en effet de reproduire la quasi-totalité du décret de 1947 en intégrant des parlementaires dans le collège. Pourtant, le passage d'un contrôle à vocation interne à un contrôle externe aurait pu induire des innovations.

Lors de la discussion parlementaire, en dehors des controverses politiques autour des récents scandales liés à l'utilisation des fonds spéciaux, les débats ont porté sur la présidence de la future commission (confiée soit à la Cour des comptes soit à un député), sur la nécessité de doter l'instance d'un secrétariat chargé de l'assister ⁽²⁾, sur celle de définir une nomenclature des pièces justificatives, sur celle de produire un rapport, mais également sur la nature parlementaire du contrôle effectué. En effet, les Sénateurs rejetaient le principe d'une habilitation ès qualités des parlementaires membres de l'instance et marquaient une réserve quant à la possibilité pour ces derniers de s'intéresser aux opérations en cours ainsi que de réaliser des enquêtes sur pièces et sur place. Le Palais du Luxembourg s'opposait donc aux attributs du contrôle parlementaire. Le dernier mot revenant à l'Assemblée nationale, la version maximaliste a recueilli la faveur des députés.

En cohérence avec les débats conduits, les sénateurs de l'opposition saisirent le Conseil constitutionnel au motif que le dispositif prévu « *encour[ai]t, sinon la censure, du moins de strictes réserves d'interprétation en ce qu'il enfrei[gna]it le principe de la séparation des pouvoirs et, en particulier, l'exclusivité des responsabilités du Président de la République et du Premier ministre en matière de défense nationale* ». Dans leur saisine, ils observaient que la désignation au sein de la commission n'était pas subordonnée à une habilitation de niveau Très Secret-Défense (laquelle suppose l'accord du Premier ministre). Ils soulignaient ensuite que la commission était appelée à obtenir communication de l'état des dépenses se rattachant à des opérations en cours, prérogative selon eux susceptible de compromettre la sécurité de celles-ci. Enfin, ils insistaient sur le fait que la nouvelle instance ne saurait confier à l'un de ses membres des pouvoirs d'enquêtes et d'investigations en vue de contrôler sur pièce et sur place les faits retracés dans les documents comptables soumis à sa vérification. Ils concluaient donc que « *[t]outes ces prérogatives sont excessives et mettent en péril la sécurité des opérations des services secrets, ainsi que, par conséquent, la séparation des pouvoirs elle-même* ⁽³⁾. »

Le Gouvernement, dans ses observations sur les recours formulés contre la loi de finances ⁽⁴⁾, rétorqua sur deux principaux points que « *la*

(1) Comme le remarque Xavier Cabannes, « *La réforme des fonds spéciaux* », *Droit et défense*, janvier 2002, p. 39.

(2) Sur ce point, un amendement du sénateur François Marc n'a hélas pas prospéré à l'Assemblée nationale.

(3) Saisine du Conseil constitutionnel en date du 20 décembre 2001 présentée par plus de soixante sénateurs, en application de l'article 61, alinéa 2, de la Constitution, et visée dans la décision no 2001-456 DC.

(4) *Journal officiel* du 29 décembre 2001.

volonté du législateur est de placer l'utilisation de ces fonds sous le contrôle du Parlement, comme dans plusieurs démocraties comparables à la France ⁽¹⁾. Cette volonté se traduit notamment par la prééminence des parlementaires dans la composition de la commission (quatre sur six) et le fait que la présidence soit confiée à l'un d'entre eux. » Dans ce cadre, selon l'exécutif, les risques pour la sécurité nationale dénoncés par les sénateurs étaient évités grâce au respect du secret de la défense nationale prévu par la loi.

En outre, le Gouvernement observait que l'objet même des investigations décrites, consistant à vérifier la conformité de l'emploi des crédits à la destination qui leur a été assignée par la loi de finances, et non à participer aux décisions prises par le pouvoir exécutif quant au choix et à la réalisation des opérations, ne pouvait pas être considéré comme une entorse au principe de séparation des pouvoirs.

En définitive, le seul point d'accord entre le Gouvernement et le Sénat résidait dans la nature parlementaire du contrôle effectué par la CVFS ⁽²⁾. Pourtant, la doctrine s'étonna de cette qualification ⁽³⁾ et s'interrogea sur l'essence de ce contrôle dès lors que le Parlement ne dispose d'aucun pouvoir de sanction, de réformation voire de recommandation publique et que la production demeure confidentielle ⁽⁴⁾. Dans le même esprit, le Livre blanc de 2008 sur la défense et la sécurité nationale rangeait la CVFS dans la catégorie des autorités administratives indépendantes ⁽⁵⁾, sans doute à bon droit au regard de sa composition hybride et de son rôle de certification des comptes.

Dans sa décision n° 2001-456 DC du 27 décembre 2001 ⁽⁶⁾, le Conseil constitutionnel s'est rangé aux arguments des sénateurs et a jugé - en s'appuyant sur l'article 35 de la Constitution - que le Parlement ne saurait intervenir dans les « opérations en cours ». La censure a également porté sur le pouvoir d'enquête conféré à la commission pour ne pas porter préjudice à ces mêmes opérations. De manière quelque peu prétorienne ⁽⁷⁾ et sans tenir compte des arguments présentés par le pouvoir exécutif lui-même, le Conseil constitutionnel a ainsi fortement borné le périmètre de ce contrôle qu'il a estimé parlementaire, l'a privé de pouvoir d'enquête et a consacré la notion

(1) À ce titre, le Gouvernement aurait pu citer le cas de l'Allemagne, où neuf membres de la commission des finances du Bundestag sont désignés à cette fin et forment « le comité de confiance ».

(2) C'est bien le Gouvernement et les parlementaires qui ont affirmé cette nature parlementaire et non le Conseil constitutionnel comme l'avance Sandrine Coursoux-Bruyère, « Les fonds spéciaux : les zones d'ombre de la réforme », *Petites affiches*, 5 janvier 2006, n°4.

(3) Cf. par exemple Xavier Cabannes, « La réforme des fonds spéciaux », article cité, p. 38.

(4) Sandrine Coursoux-Bruyère, article cité.

(5) *Défense et sécurité nationale : Le Livre blanc*, Paris, Odile Jacob, 2008, p. 140.

(6) Sans fournir plus d'explications supplémentaires que celles proposées par les sénateurs dans sa décision ou dans les commentaires publiés par la suite (in *Les Cahiers du Conseil constitutionnel*, n°12).

(7) Xavier Cabannes formule des critiques identiques in « La réforme des fonds spéciaux », article cité, note 33 p. 38. Sur cette décision, lire également Jean-Claude Zarka, « La décision du Conseil constitutionnel du 27 décembre 2001 relative à la loi de finances pour 2002 », *Recueil Dalloz*, 2002, p. 331.

« d'opération » sans que celle-ci ne jouisse d'une réelle définition juridique ⁽¹⁾.

Au final, la réforme de 2001, pourtant supposée amplifier les dispositions du décret de 1947, s'est traduite par un recul dans les capacités de contrôle des fonds spéciaux en même temps que par un élargissement de la liste des services soumis à ce contrôle. De surcroît, la composition de la CVFS a rapidement connu une évolution notoire avec le retrait des magistrats de la Cour des comptes, conformément au souhait de Philippe Séguin lorsqu'il était Premier président de la juridiction. Cette décision, sur laquelle les parlementaires membres de la Commission ont vainement tenté de le faire revenir, n'a pas été dénoncée par son successeur, Didier Migaud. Dans une lettre adressée à votre rapporteur en date du 28 avril 2015, celui-ci explicite la position de l'institution qu'il dirige : *« c'est en 2006 que mon prédécesseur a demandé la clarification des attributions respectives de cette commission et de la Cour au titre de son contrôle sur les départements ministériels ayant à gérer les fonds spéciaux. Faute de réponse du secrétariat général du Gouvernement à ses questions, et après un entretien avec M. Fromion, alors président de la commission de vérification des fonds spéciaux, mon prédécesseur a décidé qu'il ne procéderait pas au remplacement des membres sortants de la Cour au sein de la Commission »*.

3. Le contrôle des fonds spéciaux comme amplification des activités de la délégation parlementaire au renseignement (2013)

Tirant les conséquences de pareille position, les rapports de 2011 et de 2012 de la délégation parlementaire au renseignement, puis celui de la Mission d'évaluation de la Commission des lois en 2013 ⁽²⁾ préconisèrent l'absorption de la CVFS par la DPR afin d'étoffer et d'unifier le spectre du contrôle parlementaire. Le gouvernement a suivi cette préconisation et l'a matérialisée à l'occasion loi de programmation militaire examinée à la fin de l'année 2013.

Initialement envisagée, la fusion totale des deux organismes a été jugée inopportune pour deux raisons. La première tenait au fait que le fonctionnement de la CVFS est assumé par prélèvement sur les fonds spéciaux qu'elle contrôle (cette enveloppe couvre notamment les déplacements réalisés à l'étranger...). Il paraissait donc malaisé d'imaginer une absorption totale qui aurait conduit à augmenter le budget des deux chambres, à rebours des efforts de rationalisation menés par leurs présidents respectifs. En outre, il a été considéré que le principe d'une formation

(1) Par écho cependant, « on ne voit pas en quoi l'interdiction pour la commission de contrôler les opérations en cours, l'empêcherait pour les actions achevées » selon Sandrine Coursoux-Bruyère, article cité.

(2) Jean-Jacques Urvooas et Patrice Verchère, Pour un « État secret » au service de notre démocratie, Rapport d'information n° 1022, 14 mai 2013, 205 p.

spécialisée permettait de se conformer en partie aux exigences posées par le Conseil constitutionnel dans sa décision de 2001 quant à l'accès des parlementaires à des informations relatives aux opérations en cours des services de renseignement.

Néanmoins, le travail d'amendement de l'Assemblée fut conséquent sur cet article qui avait à nouveau été conçu par le Gouvernement comme une simple transposition des éléments créés en 2001. A titre d'exemple, le texte proposé à la Représentation nationale ne tenait guère compte du fait que la CVFS, bien que formation spécialisée, devenait une émanation de la DPR et qu'il était dès lors aberrant de confier sa composition aux présidents de deux chambres. L'Assemblée a préféré adopter un mode de désignation interne à la DPR, « *de manière à assurer une représentation pluraliste* », là où le Sénat avait envisagé une « *représentation de la majorité et de l'opposition* ». Or, si cette dernière est bien définie en droit parlementaire, il en va tout autrement pour la première, ce qui laissait présager pour la suite d'homériques difficultés exégétiques. De même, la désignation du président de la CVFS a-t-elle été confiée à ses membres et non aux présidents des deux chambres.

Enfin, la question de la présentation du rapport annuel a fait l'objet d'une réécriture de deux alinéas du projet de loi, synthétisés en un seul qui établit une préséance républicaine. Depuis lors, le rapport est d'abord présenté aux membres de la DPR qui n'appartiennent pas à la CVFS, puis aux présidents et rapporteurs généraux de la Commissions des finances des deux chambres, puis au président de la République et au Premier ministre. Ces deux derniers bénéficiaient auparavant d'une antériorité qui conduisait à ce que la CVFS travaillât en priorité pour l'exécutif. Pareil usage ne pouvait convenir à un organe pleinement parlementaire ⁽¹⁾.

De même, la Commission des lois de l'Assemblée nationale a été suivie lorsque, afin de ne pas entamer le rôle centralisateur du Premier ministre, il s'est agi de ne pas rendre les ministres compétents destinataires tant du rapport de la DPR que de celui de la CVFS. Pareille disposition n'est pas anodine : en effet, dans la mesure où le Premier ministre dirige en droit « *l'action du Gouvernement en matière de sécurité nationale*² » et qu'en matière de fonds spéciaux il rend les arbitrages budgétaires ultimes, il était légitime de préserver sa position non seulement en tant que chef de l'interministérialité dans le domaine du renseignement, mais aussi en tant que principal interlocuteur de la délégation et de la CVFS. Sa centralité revêt ici toute son importance dans le cadre d'une dyarchie déséquilibrée. Pour compenser le poids pris par le chef de l'État en ce domaine et assurer un contrôle

(1) Il faut d'ailleurs noter que, toujours lors de l'examen de la LPM, ces modifications protocolaires n'ont pas été acceptées dans le cas de la remise du rapport de la DPR, laquelle continue donc curieusement – au moins dans l'épure du droit – à favoriser le pouvoir exécutif à qui elle « adresse des recommandations » qu'elle « transmet » ensuite aux présidents des deux assemblées.

(2) Article L. 1131-1 du code de la défense.

parlementaire efficace, il est nécessaire que l'action gouvernementale soit réellement conduite par le chef du Gouvernement.

Article 154 tel que créé par loi de finances pour 2002 (n° 2001-1275 du 28 décembre 2001)

I. Les dépenses faites sur les crédits inscrits au chapitre 37-91 du budget des services généraux du Premier ministre sont examinées chaque année par une commission de vérification chargée de s'assurer que les crédits sont utilisés conformément à la destination qui leur a été assignée par la loi des finances.

Les services destinataires de ces crédits tiennent le compte d'emploi des fonds ainsi versés.

II. La commission est composée ainsi qu'il suit :

- deux députés, dont le président de la commission, désignés par le président de l'Assemblée nationale pour la durée de leur mandat ;
- deux sénateurs désignés par le président du Sénat après chaque renouvellement triennal ;
- deux membres nommés pour cinq ans, par décret, parmi les membres de la Cour des comptes, sur proposition de son premier président.

Sauf démission, il ne peut être mis fin aux fonctions de membre de la commission qu'en cas d'empêchement constaté par celle-ci. Les membres de la commission désignés en remplacement de ceux dont le mandat a pris fin avant son terme normal sont nommés pour la durée restant à courir dudit mandat.

III. La commission prend connaissance de tous les documents, pièces et rapports susceptibles de justifier les dépenses considérées et l'emploi des fonds correspondants. Elle se fait représenter les registres, états, journaux, décisions et toutes pièces justificatives propres à l'éclairer au cours de ses travaux de vérification.

(Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2001-456 DC du 27 décembre 2001.)

IV. Les membres de la commission sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leur mandat.

Les travaux de la commission sont secrets, sous réserve du VI.

Est puni des peines prévues à l'article 226-13 du code pénal le fait de divulguer ou publier, dans un délai de trente ans, une information relative aux travaux de la commission.

V. La commission doit avoir terminé ses travaux avant le 31 mars de l'année qui suit celle de l'exercice soumis à son contrôle.

VI. Les vérifications terminées, la commission établit un rapport sur les conditions d'emploi des crédits.

Le rapport est remis par le président de la commission au Président de la République, au Premier ministre et aux présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances.

VII. La commission dresse un procès-verbal dans lequel elle constate que les dépenses réalisées sur les crédits visés au I sont couvertes par des pièces justificatives pour un montant égal.

Le 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.

VIII. Paragraphe modificateur.

*

* *

Article 154 tel que modifié par l'article 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

I. Les dépenses faites sur les fonds spéciaux inscrits au programme intitulé : " Coordination du travail gouvernemental " sont examinées chaque année par une commission de vérification chargée de s'assurer que les crédits sont utilisés conformément à la destination qui leur a été assignée par la loi des finances.

Les services destinataires de ces crédits tiennent le compte d'emploi des fonds ainsi versés.

II.- La commission de vérification constitue une formation spécialisée de la délégation parlementaire au renseignement. Elle est composée de deux députés et de deux sénateurs, membres de la délégation parlementaire au renseignement, désignés de manière à assurer une représentation pluraliste. Le président de la commission de vérification est désigné chaque année par les membres de la délégation.

III. La commission prend connaissance de tous les documents, pièces et rapports susceptibles de justifier les dépenses considérées et l'emploi des fonds correspondants. Elle se fait représenter les registres, états, journaux, décisions et toutes pièces justificatives propres à l'éclairer au cours de ses travaux de vérification.

IV. Les membres de la commission sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leur mandat.

Les travaux de la commission sont secrets, sous réserve du VI.

Est puni des peines prévues à l'article 226-13 du code pénal le fait de divulguer ou publier, dans un délai de trente ans, une information relative aux travaux de la commission.

V. La commission doit avoir terminé ses travaux avant le 31 mars de l'année qui suit celle de l'exercice soumis à son contrôle.

VI. Les vérifications terminées, la commission établit un rapport sur les conditions d'emploi des crédits.

Le rapport est présenté aux membres de la délégation parlementaire au renseignement qui ne sont pas membres de la commission. Il 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.

VII. La commission dresse un procès-verbal dans lequel elle constate que les dépenses réalisées sur les crédits visés au I sont couvertes par des pièces justificatives pour un montant égal.

Le 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.

VII bis.- Les crédits nécessaires au fonctionnement de la commission sont inscrits au programme intitulé " Coordination du travail gouvernemental.

Le président est ordonnateur des dépenses de la commission. Il a autorité sur les agents de la commission. Les dispositions de la loi du 10 août 1922 relative à l'organisation du contrôle des dépenses engagées ne sont pas applicables aux dépenses de la commission.

VIII. (...).

En définitive, au même titre que son devancier, le contrôle parlementaire des fonds spéciaux se limite - dans les textes - à un aspect comptable puisque la commission est « *chargée de s'assurer* » que ceux-ci « *sont utilisés conformément à la destination qui leur a été assignée par la loi de finances* » ⁽¹⁾.

Il s'agit donc d'un contrôle de régularité destiné à s'assurer de la sincérité de l'imputation comptable des fonds et à vérifier que ces derniers ont bien été utilisés pour financer des dépenses qui, en raison de leur nature particulière, ne sauraient être financées par un autre truchement. Pour ce faire, la commission dispose de certaines prérogatives (dans les limites - à interroger - de la censure du Conseil constitutionnel) : toutes les informations nécessaires à sa mission doivent lui être fournies. Elle est notamment en droit de prendre connaissance de « *tous les documents, pièces et rapports susceptibles de justifier les dépenses considérées et l'emploi des fonds correspondants* ». Elle est également habilitée à se faire « *représenter les registres, états, journaux, décisions et toutes pièces justificatives propres à l'éclairer* ». Les membres de la Commission peuvent en outre se déplacer partout où sont dépensés les fonds spéciaux. A ce titre, pour cette année, la CVFS a fait le choix de réaliser des déplacements dans les pays voisins de la zone syro-irakienne.

Dans les textes, la CVFS n'assume donc pas une mission plus large de contrôle et d'évaluation des actions conduites grâce aux fonds spéciaux, ce que l'on peut déplorer tant pareille tâche s'inscrirait parfaitement dans celle dévolue à la délégation parlementaire au renseignement. Une modification du texte de loi serait donc souhaitable pour préciser cette spécificité des missions de la CVFS [**recommandation n°1**]. Au demeurant, les prérogatives de la Commission devraient être revues à l'aune des dernières évolutions constitutionnelles.

(1) Le juriste Dominique Chagnollaud l'estime d'ailleurs limité in « *Le statut des fonds spéciaux avant 2001* », Recueil Dalloz, n°21, 2014, p. 1216-1220

B. LA QUESTION DES « OPÉRATIONS EN COURS » OU LA CADUCITÉ DE LA DÉCISION DE 2001

Comme évoqué précédemment, le Conseil constitutionnel a déclaré inconstitutionnelle la faculté des membres de la CVFS à s'intéresser aux opérations en cours et à mener une enquête sur pièce et sur place concernant celles-ci. En pratique une dépense opérationnelle ne peut donc être vérifiée de manière détaillée par la Commission que dans la mesure où l'opération qu'elle finance est achevée.

Toutefois, le Conseil n'a pas pris la peine de définir ce qu'est une opération en cours, laissant pendante une question juridique déjà ancienne. En effet, si le terme « opération » est régulièrement utilisé dans des textes législatifs, il n'existe aucune définition unifiée et, surtout, aucun cadre juridique précis. De même, l'article 4 de la loi de programmation militaire pour 2014-2019 évoque des « opérations extérieures en cours » sans pour autant régler la question du déclenchement et de l'achèvement d'une opération. Au final, on peut considérer que la publication à des fins indemnitaires d'un arrêté interministériel en application de l'article L. 4123-4 du code de la défense concrétise le déclenchement d'une opération.

Consciente que le terme d'« opération » peut faire l'objet d'interprétations extensives qui auraient pour effet de priver ses contrôles de toute effectivité, la Commission a très tôt estimé qu'il convenait de lui donner une définition stricte. Elle a donc considéré que la notion d'« opération » recouvre un ensemble d'actions menées en vue d'obtenir un résultat opérationnel déterminé. Lorsque ce résultat est atteint, elle estime avoir *de jure* accès aux pièces relatives à cet ensemble d'actions.

Jusqu'à cette année, la Commission n'avait jamais rencontré de point de désaccord avec les services tributaires sur le périmètre de son contrôle¹ (il lui a été opposé un refus de communication). Quoi qu'il en soit, la Commission invite les directeurs de service à formaliser par une décision signée de leur main ou de la main de leurs (sous-)directeurs le déclenchement et l'achèvement d'une opération. Cette démarche aurait pour effet de restreindre la notion d'opération (trop souvent employé comme synonyme de « mission ») [**recommandation n°2**]. La CVFS considère pour sa part que la transmission de pièces comptables au service de contrôle interne de chaque administration du renseignement lui permet d'entamer sa mission de contrôle. Or, elle appelle à une transmission mensuelle.

De surcroît, la Commission estime que le refus de communication de pièces justificatives en raison du non achèvement d'une mission n'a plus de bien-fondé juridique depuis la révision constitutionnelle de 2008. De fait,

(1) Cf. par exemple le témoignage d'un ancien président de la CVFS René Galy-Dejean, *Circonstances et convictions*, Paris, Numéris, 2007.

celle-ci a modifié de manière conséquente les articles sur lesquels le Conseil constitutionnel a fondé sa décision de 2001.

En effet, le Conseil a principalement appuyé sa décision sur l'article 35 de la Constitution ⁽¹⁾ qui disposait jusqu'à la réforme : « *La déclaration de guerre est autorisée par le Parlement* ».

La révision de 2008 a permis d'adopter une version plus étoffée : « *La déclaration de guerre est autorisée par le Parlement*.

Le Gouvernement informe le Parlement de sa décision de faire intervenir les forces armées à l'étranger, au plus tard trois jours après le début de l'intervention. Il précise les objectifs poursuivis. Cette information peut donner lieu à un débat qui n'est suivi d'aucun vote.

Lorsque la durée de l'intervention excède quatre mois, le Gouvernement soumet sa prolongation à l'autorisation du Parlement. Il peut demander à l'Assemblée nationale de décider en dernier ressort.

Si le Parlement n'est pas en session à l'expiration du délai de quatre mois, il se prononce à l'ouverture de la session suivante ».

Le but consistait à renforcer le contrôle parlementaire comme l'avait clairement énoncé Hervé Morin, alors ministre de la Défense, lors des débats parlementaires : « *Le souhait du Gouvernement, qui a été confirmé devant le Conseil d'État, est de concentrer le contrôle sur l'envoi des militaires en corps constitués à des fins opérationnelles* ⁽²⁾ ». Ainsi, et quelles que soient les modalités de l'information, le Parlement est-il désormais informé des opérations extérieures en cours, à rebours de la jurisprudence du Conseil. Ce dernier a d'ailleurs reconnu les changements opérés dans la décision n° 2009-582 DC du 25 juin 2009 (considérant n° 30 et son commentaire aux Cahiers n° 7). C'est dans ce nouveau cadre que l'article 4 de la LPM 2014-2019 peut avancer sans redouter la censure : « *Les opérations extérieures en cours font, chaque année, l'objet d'un débat au Parlement. Le Gouvernement communique, préalablement à ce débat, aux commissions compétentes de l'Assemblée nationale et du Sénat un bilan politique, opérationnel et financier des opérations extérieures en*

(1) Cf. les considérants 44 et 45 de la décision n° 2001-456 DC du 27 décembre 2001 : « 44. Considérant qu'aux termes du second alinéa de l'article 5 de la Constitution, le Président de la République "est garant de l'indépendance nationale, de l'intégrité du territoire et du respect des traités" ; qu'en vertu de son article 15, il est "le chef des Armées" ; que son article 21 dispose que le Premier ministre "est responsable de la Défense Nationale" ; qu'aux termes de son article 35, le Parlement autorise la déclaration de guerre ; qu'en application de ses articles 34 et 47, le Parlement vote, à l'occasion de l'adoption des lois de finances, les crédits nécessaires à la défense nationale ;

45. Considérant qu'il résulte de l'ensemble des dispositions constitutionnelles précitées que, s'il appartient au Parlement d'autoriser la déclaration de guerre, de voter les crédits nécessaires à la défense nationale et de contrôler l'usage qui en a été fait, il ne saurait en revanche, en la matière, intervenir dans la réalisation d'opérations en cours ; qu'il y a lieu, dès lors, de déclarer contraires à la Constitution les dispositions de l'avant-dernier alinéa du III de l'article 154 et de son dernier alinéa qui en est inséparable ; »

(2) Intervention du 27 mai 2008 à l'Assemblée Nationale du ministre de la défense sur l'article 13 de la loi constitutionnelle.

cours. » En outre, les parlementaires des commissions de la Défense des deux assemblées ont pris l'habitude d'envoyer des délégations auprès des forces armées déployées opérations extérieures afin d'informer les assemblées sur la pertinence politique et stratégique des engagements extérieurs et de contrôler l'adéquation des moyens mis en œuvre pour atteindre les objectifs fixés par l'exécutif.

Au regard de ces développements, la CVFS ne s'estime plus liée par une interdiction générale de prendre connaissance d'une opération en cours **[recommandation n°3]**. Elle retient cependant la nécessité que son contrôle ne puisse en aucun cas entraver le bon déroulement de l'activité opérationnelle des services (souci évident et légitime du Conseil constitutionnel en 2001) et juge à cet effet que les enquêtes sur pièces et sur place ne sauraient porter sur ces opérations **[recommandation n°4]**. Ces considérations invitent d'ailleurs à plaider en faveur d'une modification de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, lequel définit les prérogatives de la DPR. En effet, la restriction posée concernant les opérations en cours n'a plus lieu d'être **[recommandation n°5]**.

C. QUELS MOYENS POUR LE CONTRÔLE DES FONDS SPÉCIAUX ? UNE NÉCESSAIRE RÉVISION LÉGISLATIVE

Si la CVFS dispose de prérogatives étendues, la question des finalités du contrôle opéré, de son étendue (cf. ci-avant) ainsi que des moyens humains et matériels revêt une importance cardinale.

Comme l'a évoqué la doctrine, la loi ne prévoit aucun pouvoir de sanction ou de réformation ni même de recommandation publique ou de mise en garde. Toutefois, depuis 2001, les recommandations de la Commission ont été scrupuleusement suivies par les services de renseignement qui en sont destinataires. Au demeurant, si des manquements devaient être constatés, la délégation parlementaire au renseignement pourrait désormais prendre toutes les mesures nécessaires pour alerter le Gouvernement et faire jouer la responsabilité politique de celui-ci. En outre, les parlementaires votent chaque année les dotations budgétaires et un débat public pourrait faire état des réserves de l'instance parlementaire chargée de leur contrôle. Enfin, la nouvelle publicité de l'action conduite par la CVFS constituera indéniablement un pouvoir supplémentaire qui répond aux observations doctrinales pleinement justifiées ; elle s'inscrira pleinement dans la philosophie du contrôle parlementaire.

Cependant, la question des moyens humains affectés à ce contrôle se repose avec une grande acuité : en effet, contrairement à ce que pourrait laisser entendre l'article 154 précité en son VII bis, la Commission ne dispose pas de personnels dédiés et s'appuie donc sur les administrateurs que les commissions des finances et de la défense de l'Assemblée nationale et du

Sénat délèguent à cet effet. Mais le contrôle des fonds vient s'ajouter à leurs activités habituelles, déjà fort conséquentes.

En plus de ces trois administrateurs, pour la première fois, un collaborateur parlementaire disposant des habilitations nécessaires s'est adjoint aux équipes administratives. La CVFS a en cela imité les dispositifs allemand et états-unien de contrôle parlementaire du renseignement : dans ces deux pays, les parlementaires dédient une partie de leurs équipes - infiniment plus étoffées qu'en France - à ces missions essentielles.

Au cours de cette année, comme c'est le cas depuis quatorze ans, les agents de la Commission ont réalisé des inspections préalables aux visites de contrôle menées par les parlementaires afin d'assurer un contrôle exhaustif des masses financières concernées. Ces mêmes agents ont accompagné les membres de la CVFS dans leurs déplacements à l'étranger. Toutefois, pour la première fois depuis 2001, et à rebours de la coutume établie, les collaborateurs d'un ministre de la communauté du renseignement se sont opposés à ce que les agents réalisent les travaux préparatoires mentionnés ci-avant hors la présence des parlementaires. Pareille position s'appuie sur une interprétation restrictive - et discutable - de la loi de 2001 ; elle s'inscrit d'ailleurs en contradiction avec les intentions du législateur qui avait renoncé à créer un secrétariat dans la mesure où ces précisions étaient à l'époque jugées superflues. Elle s'écarte enfin des pratiques observées au sein de toutes les nations occidentales où les agents assistent et représentent les élus dans leurs activités dans la mesure où aucun parlementaire ne réalise à temps plein sa mission de contrôle en raison des autres obligations qui pèsent sur lui (travail de commission, rapports législatifs, missions d'informations, votes, autres missions de contrôle...).

Si la CVFS a pu achever sa mission de contrôle dans les mêmes conditions qu'auparavant, elle prend acte de l'interprétation du Gouvernement et de sa volonté de réglementer drastiquement les modalités de contrôle pour l'année prochaine. Ces changements soudains la conduisent à militer en faveur d'une modification de la loi qui tiendrait d'ailleurs compte des recommandations précédentes [**recommandation n°6**]. Le tableau qui suit synthétise et explicite les modifications législatives souhaitées.

De surcroît, et au-delà de cet aspect déterminant, ces moyens à temps partiel paraissent très insuffisants au regard des exigences du contrôle à effectuer, du temps à y consacrer... De fait, la CVFS souhaiterait qu'au moins un administrateur des assemblées parlementaires soit affecté à plein temps à son service [**recommandation n°7**]. De même, elle préconise de solliciter la Cour des comptes afin que celle-ci désigne des magistrats pour assister le travail de la Commission en application de l'article 47-2 de la Constitution [**recommandation n°8**]. La CVFS salue d'ailleurs la proposition formulée en ce sens par le Premier président Migaud dans la lettre

précédemment citée. De ce fait, l'ensemble de ces personnels serait à même de réaliser un travail de vérification tout au long de l'année.

Enfin, la Commission estime nécessaire de conduire une réflexion sur son budget de fonctionnement [**recommandation n°9**] : il lui semble surprenant que ses frais soient imputés sur les fonds spéciaux qu'elle contrôle et appelle de ses vœux la création d'une ligne autonome au sein des budgets des assemblées parlementaires. Car, il importe de pouvoir engager des dépenses (correspondant, notamment, aux déplacements effectués par ses membres) sans recourir à l'entremise du pouvoir exécutif comme c'est aujourd'hui le cas.

Tableau 2 : Synthèse des modifications législatives souhaitées pour un contrôle des fonds spéciaux plus efficace

Texte actuel	Modifications proposées	Commentaires
	<p>I. Les fonds spéciaux inscrits au programme « Coordination du travail gouvernemental » sont, chaque année, répartis et mis à la disposition des services désignés par arrêté non publié du Premier ministre, sous la forme de dotations.</p> <p>Les crédits disponibles en fin d'année sur l'une de ces dotations peuvent être reportés l'année suivante sur la même dotation, dans la limite de 15 % des crédits initiaux inscrits sur la dotation à partir de laquelle les crédits sont reportés.</p>	<p>Cet ajout au texte initial a pour objectif de rappeler le rôle du Premier ministre dans les arbitrages budgétaires rendus.</p> <p>Il entend aussi prévoir une dérogation au principe d'annualité budgétaire afin de permettre au service de conserver des reliquats qui n'excèdent pas 15% de leur dotation annuelle, comme c'est le cas aujourd'hui sans réelle base légale (cf. la partie II).</p>
<p>I. Les dépenses faites sur les fonds spéciaux inscrits au programme intitulé : " Coordination du travail gouvernemental " sont examinées chaque année par une commission de vérification chargée de s'assurer que les crédits sont utilisés conformément à la destination qui leur a été assignée par la loi des finances.</p> <p>Les services destinataires de ces crédits tiennent le compte d'emploi des fonds ainsi versés.</p>	<p>Ces services tiennent le compte d'emploi des dotations reçues.</p> <p>Les dépenses financées sur ces dotations sont soumises chaque année au contrôle et à l'évaluation d'une commission de vérification chargée de s'assurer que les crédits sont notamment utilisés conformément à la destination qui leur a été assignée par la loi de finances.</p> <p>Ce contrôle porte sur les exercices clos.</p>	<p>Au-delà de l'inversion d'un alinéa modifié pour des raisons de pure forme, la modification préconisée introduit la notion de « contrôle et d'évaluation » propre au contrôle parlementaire tel que prévu par l'article 24 de la Constitution. Elle précise également que l'activité de la CVFS porte sur l'année écoulée et non celle en cours (ce qui diminue d'ailleurs le risque d'avoir à connaître d'opérations en cours).</p>
<p>II.- La commission de vérification constitue une formation spécialisée de la délégation parlementaire au renseignement. Elle est composée de deux députés et de deux sénateurs, membres de la délégation parlementaire au renseignement, désignés de manière à assurer une</p>		

<p>représentation pluraliste. Le président de la commission de vérification est désigné chaque année par les membres de la délégation.</p>		
<p>III. La commission prend connaissance de tous les documents, pièces et rapports susceptibles de justifier les dépenses considérées et l'emploi des fonds correspondants.</p>		
<p>Elle se fait représenter les registres, états, journaux, décisions et toutes pièces justificatives propres à l'éclairer au cours de ses travaux de vérification.</p>	<p>Elle se fait représenter tous les documents, rapports et pièces justificatives susceptibles de l'éclairer au cours de ses travaux de vérification, y compris lorsque ceux-ci concernent des opérations en cours déclenchées lors de l'exercice soumis à son contrôle.</p> <p>Elle peut procéder à toutes enquêtes et investigations en vue de contrôler les faits retracés dans les documents comptables soumis à sa vérification à l'exception de ceux concernant des opérations en cours.</p>	<p>Conformément à l'analyse constitutionnelle réalisée ci-avant, la CVFS souhaite réintroduire la notion d'opérations en cours censurée en 2001 ainsi que la capacité d'enquête sur pièces et sur place (laquelle correspond à la réalité des pratiques actuelles). Elle exclut toutefois les opérations en cours dans ce cadre afin de ne pas nuire à leur bon déroulement.</p>
<p>IV. Les membres de la commission sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leur mandat.</p>	<p>IV. Les membres de la commission, comme les agents désignés pour les assister ou les représenter, sont astreints au respect du secret de la défense nationale protégé en application des articles 413-9 et suivants du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance à raison de leur mandat.</p> <p>Les agents mentionnés à l'alinéa précédent doivent être habilités au secret de la défense nationale aux fins d'accéder aux informations et aux documents nécessaires à l'accomplissement de leur mission.</p>	<p>Par la mention des « agents désignés pour les assister ou les représenter », la CVFS entend résoudre la controverse juridique qui l'oppose au Gouvernement. Elle prévoit naturellement l'habilitation des agents concernés, comme c'est aujourd'hui le cas.</p>

<p>Les travaux de la commission sont secrets, sous réserve du VI.</p> <p>Est puni des peines prévues à l'article 226-13 du code pénal le fait de divulguer ou publier, dans un délai de trente ans, une information relative aux travaux de la commission.</p>		
<p>V. La commission doit avoir terminé ses travaux avant le 31 mars de l'année qui suit celle de l'exercice soumis à son contrôle.</p>	<p>suppression</p>	<p>Depuis 2001, le contrôle de la CVFS s'exerce sur des années pleines ; une date de remise du rapport paraît dès lors superflue ; elle peut même constituer une entrave. La seule obligation légale doit résider dans la publication d'un rapport annuel.</p>
<p>VI. Les vérifications terminées, la commission établit un rapport sur les conditions d'emploi des crédits.</p>	<p>VI. Les vérifications terminées, la commission établit chaque année un rapport sur les conditions d'emploi des crédits.</p>	
<p>Le rapport est présenté aux membres de la délégation parlementaire au renseignement qui ne sont pas membres de la commission. Il est également remis, par le président de la délégation, aux présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargés des finances ainsi qu'au Président de la République et au Premier ministre.</p>		
	<p>Dans le respect du secret de la défense nationale, la commission peut établir un rapport public.</p>	<p>Cet ajout entérinerait la pratique initiée par le présent rapport.</p>
<p>VII. La commission dresse un procès-verbal dans lequel elle constate que les dépenses réalisées sur les crédits visés au I sont couvertes par des pièces justificatives pour un montant égal.</p> <p>Le 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.</p> <p>VII bis.- Les crédits nécessaires au fonctionnement de la commission sont inscrits au programme intitulé " Coordination du travail gouvernemental.</p> <p>Le président est ordonnateur des dépenses de la commission. Il a autorité sur les agents de la commission. Les dispositions de la loi du 10 août 1922 relative à l'organisation du contrôle des dépenses engagées ne sont pas applicables aux dépenses de la commission.</p> <p>VIII. Paragraphe modificateur.</p>		

II. ELÉMENTS DE SYNTHÈSE PUBLIQUE EXTRAITS DES PROCÈS-VERBAUX

Comme évoqué précédemment, le présent rapport public s'accompagne de procès-verbaux adressés à chaque service récipiendaire afin de réaliser un compte-rendu des missions de contrôle effectuées et spécifier pour chaque administration les préconisations formulées par la Commission. Seul un résumé non confidentiel sera ici publié.

A. POUR UNE REVALORISATION DU BUDGET DES FONDS SPÉCIAUX

La CVFS, dans le cadre de ses missions de contrôle, a pu constater que l'emploi des fonds spéciaux répondait – à de très rares et mineures exceptions – à la doctrine qu'elle a élaborée depuis 14 ans, à savoir que ces dotations ne sauraient être utilisées dans un autre objectif que le financement d'activités nécessitant de rester confidentielles ou requérant une grande réactivité opérationnelle. Ces considérations conduisent d'ailleurs à marquer un réel étonnement concernant la stabilité de l'enveloppe consacrée aux fonds spéciaux : alors que les budgets octroyés aux services de renseignement ont connu une progression appréciable et conforme à la reconnaissance de la fonction stratégique assumée ainsi qu'à la hausse de leur activité, la Commission constate que les fonds spéciaux n'ont pas bénéficié d'une revalorisation alors même qu'ils financent la partie la plus sensible de l'activité de ces administrations. Elle attire donc l'attention du Premier ministre sur l'impérieuse nécessité de revaloriser au moins à hauteur de 50% le montant octroyé aux services de renseignement **[recommandation n°10]**.

B. POUR UN USAGE RATIONALISÉ DES FONDS SPÉCIAUX

Pareille revalorisation viendrait en soutien d'un surcroît d'activité opérationnelle ou 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 **[recommandation n°11]**. Elle répondrait également aux coûts croissants qu'engendrent la recherche de l'anonymat ou la préservation de la confidentialité de certaines actions. Elle permettrait enfin de tenir compte de la constitution d'un deuxième cercle de la communauté du renseignement composé notamment du Service central du renseignement territorial (SCRT), de la Direction du renseignement de la préfecture de police (DRPP) et de la Sous-direction à l'anticipation opérationnelle de la Gendarmerie nationale (SDAO). Certains de ces services pourraient ainsi être

destinataires d'une dotation destinée à financer leur action qui s'inscrit en soutien des services du premier cercle [**recommandation n°12**]. De fait, la CVFS estime que l'accès de ces services aux techniques de recueil du renseignement, témoignage de leur contribution au renseignement de souveraineté, doit logiquement s'accompagner d'une dotation en fonds spéciaux.

Néanmoins, la Commission souhaite que l'octroi de fonds spéciaux réponde à une activité opérationnelle et des projets budgétés avec soin et non à une routine administrative [**recommandation n°13**]. Dans cet esprit, elle rappelle qu'aucune dérogation autre que coutumière n'a été instaurée au principe d'annualité budgétaire des fonds spéciaux (une modification législative serait en ce sens souhaitable ⁽¹⁾, cf. les propositions formulées dans le tableau ci-avant) [**recommandation n°14**]. Dès lors, elle juge que la constitution d'importants reliquats au sein des services s'écarte de l'épure du droit et des règles de bonne gestion lorsqu'ils représentent une part trop significative de la dotation annuelle [**recommandation n°15**]. En effet, la CVFS comprend la nécessité de conserver une trésorerie afin de faire face à des imprévus ou des versements qui interviennent à échéance du premier trimestre de l'année, mais elle souhaite que celle-ci soit contenue. Elle estime que la non consommation des crédits par un service récipiendaire doit conduire le Premier ministre à examiner la nature de la demande budgétaire réalisée et à s'assurer qu'elle vient en appui à des activités constatées ou des projets formulés.

Cette rigueur budgétaire implique nécessairement de nouvelles modalités de gestion des fonds spéciaux qui devraient passer par un dialogue plus soutenu avec les services du Premier ministre ainsi qu'une parfaite réactivité de leur part. Ainsi la CVFS souhaite-t-elle que les premiers versements en fonds spéciaux interviennent dès la fin du mois de janvier [**recommandation n°16**]. En outre, elle plaide en faveur de la constitution d'une enveloppe de précaution afin de faire face à des sollicitations imprévues [**recommandation n°17**]. Si cette option n'était pas retenue, elle sollicite un recours plus aisé aux décrets de dépenses accidentelles et imprévisibles (DDAI) au profit de tous les services de la communauté du renseignement lorsqu'ils sont confrontés à des impératifs opérationnels soudains [**recommandation n°17 bis**]. La question du montant de ces DDAI comme facteur d'éligibilité ne lui paraît pas pertinente au regard d'exemples passés.

(1) Jusqu'à la réforme de 2001, les crédits inusités devaient être annulés pour être reversés au budget général en application de l'article 42 de loi de 1946 (sur ce point, se référer à David Biroste, « Les fonds spéciaux : contribution à l'étude des marges du droit (seconde partie) », *Revue française de finances publiques*, mars 2003, n°81, p. 315). Mais cette règle n'était pas appliquée comme l'évoque le rapport Logerot, *op. cit.*, p. 9.

C. LA QUESTION DES DDAI

Au demeurant, la Commission s'interroge sur le recours routinisé aux DDAI afin de financer les dépenses de certains services de la communauté du renseignement.

Conçus pour faire face à des dépenses urgentes et imprévisibles telles les catastrophes naturelles ou sanitaires, ces décrets sont pris en application du programme budgétaire 552 (*Dépenses accidentelles et imprévisibles*), l'une des deux composantes de la mission *Provisions*. Ce programme se caractérise par une souplesse avantageuse : contrairement aux autres leviers d'aménagements budgétaires à disposition de l'exécutif (loi de finances rectificative, décrets d'avance, virements et transferts entre programmes, dégel de crédits mis en réserve) qui supposent de recueillir l'avis et/ou l'accord de différentes institutions, les DDAI ne sont pas soumis aux mêmes obligations. En effet, les fonds affectés au programme 552 relèvent d'un simple décret du Premier Ministre pris sur rapport du ministre chargé des Finances. Ces documents ne font pas nécessairement l'objet d'une publication, notamment lorsqu'ils relèvent de la Défense nationale. Ils sont d'ailleurs fréquemment utilisés pour financer des opérations extérieures, s'éloignant quelque peu de l'épuration du droit selon la Cour des comptes. Dans le même ordre d'idées, ils ont permis, depuis 2009, d'acquérir un immeuble, de financer la campagne de vaccination contre le virus H1N1, de consulter les habitants sur le projet du Grand Paris, de payer des crédits de personnel en fin d'année...

En sus de sa souplesse, le programme se caractérise par l'absence d'évaluation et de contrôle prévus par la LOLF au regard des objectifs poursuivis (parer à l'imprévisible). Seul le contrôle des fonds spéciaux, lorsque des DDAI concernent des services de renseignement, introduit une nuance à ce propos.

Ces caractéristiques particulières ont conduit la Cour des comptes à proposer de préciser la doctrine d'emploi de ces fonds afin de les cantonner « *aux situations de calamités ou aux dépenses réellement imprévisibles* ». La Cour poursuit : « *L'absence de doctrine d'emploi, la faiblesse des montants inscrits sur la mission et l'existence d'autres dispositifs permettant de faire face à des dépenses urgentes et imprévues (mise en réserve, auto-assurance) conduisent à mettre en question l'utilité de la mission.* » Ces positions sont réaffirmées chaque année dans le rapport sur *l'exécution du budget de l'Etat par mission et programme*.

Dans le domaine du renseignement, la CVFS a constaté le recours systématique à des DDAI afin de financer, au-delà du déclenchement de la crise, des dépenses qui, avec le temps, deviennent prévisibles. La Commission s'interroge sur cette pratique et se demande en particulier si elle ne constitue pas la contrepartie d'une volonté de maintenir une dotation en fonds spéciaux gelée. Or, si l'on omet la réelle complexité comptable introduite, 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 immuable dotation en fonds spéciaux de nouvelles dépenses qui supposent d'autres économies parfois préjudiciables. En conséquence, la Commission réaffirme son désir de voir la dotation en fonds spéciaux accrue de manière conséquente afin d'intégrer le montant cumulé des DDAI et d'offrir aux services concernés une gestion plus saine et sereine de leurs budgets sur le moyen terme. Pareille décision permettra de limiter le recours aux DDAI et de le restreindre à son objet principal : la gestion temporaire de l'imprévisible [**recommandation n°18**]. Cependant, l'accroissement souhaité de l'enveloppe ne saurait se limiter à la seule prise en compte des DDAI mais doit au contraire aller au-delà.

D. REVOIR LES MÉCANISMES D'ATTRIBUTION DES FONDS SPÉCIAUX

De jure, le Premier ministre rend les arbitrages budgétaires qui président à la répartition des fonds spéciaux entre les services de renseignement. Toutefois, le Coordonnateur national du renseignement, collaborateur du Président de la République, joue naturellement le rôle de centralisateur des demandes formulées par les services. Par ce biais, il réalise en réalité le premier arbitrage budgétaire qui s'avérera déterminant, le cabinet du Premier ministre s'écartant rarement des préconisations de celui qui paraît le mieux placé pour évaluer les besoins financiers des administrations concernées.

Aussi l'idée de rattacher le Coordonnateur national du renseignement tant à l'Élysée qu'à Matignon se révèle-t-elle séduisante (en le nommant par exemple conseiller renseignement du Premier ministre à l'image de pratiques qui ont déjà eu cours). Des rapports parlementaires ont précédemment formulé des recommandations en ce sens ⁽¹⁾. Il s'agirait non de le détacher du chef de l'État mais plutôt de le rapprocher du chef du Gouvernement. Le Coordonnateur serait concomitamment le collaborateur des deux têtes de l'exécutif.

En effet, comment continuer à ignorer son rattachement pour le moins baroque ? Ainsi, selon le décret n° 2010-299 du 22 mars 2010, le Coordonnateur et son équipe relèvent-ils « *pour [leur] gestion administrative et financière* » du Secrétariat général du gouvernement, donc du Premier ministre, alors même que le Président de la République est le principal bénéficiaire de leur action. Une telle évolution permettrait de lui confier d'utiles capacités d'arbitrages budgétaires, ainsi que l'évoque le Livre blanc de 2013 ⁽²⁾. Si les arguments avancés n'ont jusqu'à présent pas porté, la CVFS

(1) Sur ce point, se référer au rapport de Jean-Jacques Urvoas et Patrice Verchère, *op. cit.*, p. 108 et s. ainsi qu'au rapport public de la Délégation parlementaire au renseignement pour l'année 2014, p. 22-23.

(2) Livre blanc : *Défense et sécurité nationale*, Paris, La Documentation Française, 2013, p. 71

ne désespère pas d'inspirer une modification de l'article R*1122-8 du code de la défense [**recommandation n°19**].

E. VERS UNE STANDARDISATION DE LA GESTION DES FONDS SPÉCIAUX

Les diverses missions de contrôle réalisées par la Commission en France et à l'étranger ont globalement démontré la rigueur de gestion des fonds spéciaux. Même si les compliments peuvent paraître convenus et dissonants au sein d'un rapport parlementaire, la CVFS tient à saluer l'implication personnelle des agents concernés, leur professionnalisme et leur sens du devoir.

En dépit de ce constat, et au-delà des contingences liées aux particularités de chacune des administrations contrôlées, la Commission a notamment souhaité promouvoir une nomenclature unique des pièces justificatives et modes de comptabilité afin de faciliter et d'unifier le contrôle mais également la gestion interne [**recommandation n°20**]. Pareille lacune avait été déplorée à juste titre lors des débats fondateurs de 2001 ; le temps passé et l'expérience accumulée permettent aujourd'hui d'y remédier. La CVFS souhaite dans cet esprit que le Coordonnateur national du renseignement œuvre à la diffusion des bonnes pratiques et à la sensibilisation des acteurs (y compris par la diffusion d'une directive s'inspirant des préconisations de la Commission) [**recommandation n°21**].

Car la CVFS insiste sur la nécessité de respecter ces règles de gestion qui, au-delà du formalisme apparent, assurent une utilisation conforme des fonds spéciaux et apportent une réelle plus-value dans l'activité du service (contrôle interne, évaluation de l'efficacité...). Elle porte en effet une attention soutenue aux mécanismes de contrôle interne dont elle estime le renforcement nécessaire conformément à des recommandations déjà réalisées dans des documents parlementaires ⁽¹⁾ [**recommandation n°22**].

La Commission de vérification des fonds spéciaux, quelles que soient les critiques ou recommandations formulées, se félicite des efforts appliqués dans la gestion des fonds spéciaux. Elle milite pour une démarche ambitieuse et moderne en ce domaine stratégique trop souvent oublié des commentateurs en raison de sa confidentialité. Elle espère que ce premier rapport public contribuera à cette ambition.

(1) Sur ce point, se référer au rapport de Jean-Jacques Urvoas et Patrice Verchère, *op. cit.*, p. 54 et s. ainsi qu'au rapport public de la Délégation parlementaire au renseignement pour l'année 2014, p. 70 et s.

CONCLUSION

La publication d'un premier rapport public représente toujours une étape majeure dans la vie d'une instance de contrôle, surtout lorsque celle-ci existe depuis quatorze ans et a toujours fonctionné dans la plus parfaite discrétion. Mais, comme évoqué précédemment, le regard du public n'est pas incompatible avec la préservation du secret de la défense nationale. L'existence de ce dernier n'a d'ailleurs de sens que si le premier peut aller aussi loin que possible. Car les services de renseignement agissent pour la sécurité de nos concitoyens et la préservation du cadre démocratique de notre régime. Loin d'être un instrument de la Raison d'État ou d'un quelconque « État profond », ils incarnent un outil de souveraineté soumis à une pluralité de contrôles complémentaires et rigoureux.

En ce sens, le présent rapport a formulé 22 recommandations dont la mise en œuvre paraît nécessaire à la poursuite d'un contrôle efficace et d'une utilisation optimale des fonds spéciaux. Elles viennent compléter la centaine de recommandations formulées dans les procès-verbaux adressés aux services de renseignement et à l'exécutif. La CVFS sera attentive à leur prise en compte et en effectuera un suivi minutieux.

En effet, les objectifs poursuivis par le contrôleur et le contrôlé coïncident parfaitement dans la mesure où ils s'inscrivent au service de la Nation. Il importe dès lors que le dialogue se poursuive pour tendre vers un perfectionnement continu.

La modernité et les exigences de nos concitoyens imposent un cadre d'action étroit et exigeant pour nos services. La noblesse de leur métier découle de cette tension qui nécessite également une meilleure connaissance de cette sphère d'action trop souvent caricaturée ou objet de phantasmes. Or contrôler et comprendre le contrôle supposent de connaître. Pour ce faire, œuvrer à la diffusion d'une culture française du renseignement s'impose comme un absolu. La Commission de vérification des fonds spéciaux a souhaité apporter sa pierre à un édifice dont les fondations ne sont pas achevées.

RELEVÉ DES RECOMMANDATIONS DE LA CVFS

Recommandation n°1 : Consacrer dans la loi la fonction de contrôle et d'évaluation des fonds spéciaux conférée à la CVFS ;

Recommandation n°2 : Inciter les directeurs de service à formaliser par une décision signée de leur main ou de la main de leurs (sous-)directeurs le déclenchement et l'achèvement d'une opération ;

Recommandation n°3 et 5 : Abolir, pour la CVFS et la DPR, la restriction des « opérations en cours » au regard des évolutions constitutionnelles survenues en 2008 ;

Recommandation n°4 : Exclure du champ des enquêtes sur pièces et sur place les opérations en cours ;

Recommandation n°6 : Modifier en profondeur les dispositions législatives relatives à la CVFS (missions, moyens, période de contrôle, publication d'un rapport) ;

Recommandation n°7 : Affecter à la CVFS un administrateur des services de l'Assemblée nationale et/ou du Sénat à temps plein ;

Recommandation n°8 : Solliciter le concours de la Cour des comptes ;

Recommandation n°9 : Conduire une réflexion sur le budget de fonctionnement de la CVFS ;

Recommandation n°10 : Revaloriser au moins à hauteur de 50% la dotation en fonds spéciaux octroyée aux services de renseignement ;

Recommandation n°11 : Anticiper les menaces à venir et dégager les moyens financiers nécessaires pour les entraver ;

Recommandation n°12 : Octroyer une dotation en fonds spéciaux à certains services du deuxième cercle de la communauté du renseignement ;

Recommandation n°13 : N'octroyer une dotation en fonds spéciaux qu'en réponse à une expression de besoins détaillée et budgétée ;

Recommandation n°14 : Prévoir dans la loi une dérogation au principe d'annualité budgétaire ;

Recommandation n°15 : Limiter le reliquat conservé par les services destinataires au strict nécessaire ;

Recommandation n°16 : Verser la première tranche de la dotation en fonds spéciaux dès le mois de janvier ;

Recommandation n°17 : Constituer une enveloppe de précaution afin de faire face à des sollicitations imprévues ;

Recommandation n°17 bis : Permettre un recours plus aisé aux décrets de dépenses accidentelles et imprévisibles (DDAI) au profit de tous les services de la communauté du renseignement lorsqu'ils sont confrontés à des impératifs opérationnels soudains ;

Recommandation n°18 : Limiter le recours aux DDAI au profit d'un accroissement pérenne des dotations en fonds spéciaux ;

Recommandation n°19 : Modifier le code de la défense afin de consacrer un rattachement du Coordonnateur national du renseignement à la fois au Président de la République et au Premier ministre afin de lui permettre notamment de réaliser des arbitrages budgétaires ;

Recommandation n°20 : Promouvoir une nomenclature unique des pièces justificatives et modes de comptabilité afin de faciliter et d'unifier le contrôle mais également la gestion interne ;

Recommandation n°21 : Œuvrer à la diffusion des bonnes pratiques et à la sensibilisation des acteurs (y compris par la diffusion d'une directive du CNR s'inspirant des préconisations de la CVFS) ;

Recommandation n°22 : Renforcer les mécanismes de contrôle interne au sein des services de renseignement.

EXAMEN PAR LA DÉLÉGATION

Réunie le jeudi 14 janvier 2015 sous la présidence de M. Jean-Pierre Raffarin, président, la délégation a procédé à l'examen du rapport annuel. Après un exposé de son président-rapporteur, la délégation a adopté son rapport pour 2015 (chapitre 1 à 4), en application du VI de l'article 6 nonies de l'ordonnance n°58-1100 du 17 novembre 1958.

Elle a ensuite entendu 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).

LES PROPOSITIONS DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT

I. PROPOSITIONS CONCERNANT LA MISE EN ŒUVRE DE LA LOI SUR LE RENSEIGNEMENT

1/ Affecter au GIC les personnels mis à disposition par le ministère de la défense avant le 31 décembre 2017.

2/ Attribuer au GIC du statut de service à compétence nationale.

3/ Rendre l'arbitrage technique *** dans les meilleurs délais.

4/ Mettre en œuvre sans retard les techniques de renseignement *** eu égard *** au niveau de la menace terroriste.

5/ Permettre à la CNCTR de disposer d'un accès permanent, complet et direct aux éléments collectés par les nouvelles techniques dans les conditions posées par la loi et dans des délais raisonnables.

6/ Exercer un contrôle vigilant sur les demandes des services habilités à utiliser les nouvelles techniques de renseignement par le décret du 11 décembre 2015 dont le renseignement ne constitue pas la spécialité. La DPR recommande aux ministres concernés et à leurs délégués une vigilance particulière lorsqu'ils seront amenés à examiner ces demandes, de vérifier s'ils disposent des compétences techniques requises et s'ils ont mis en place des dispositifs de contrôle interne rigoureux. Elle demande au Premier ministre et à ses délégués d'assurer un contrôle vigilant lorsqu'ils devront procéder à l'examen des demandes présentées.

7/ Mettre en place un contrôle administratif renforcé au sein des services de renseignement et au sein des services habilités à utiliser les nouvelles techniques de renseignement par le décret du 11 décembre 2015.

8/ Demander à l'inspection des services de renseignement de proposer dans les meilleurs délais un standard commun de contrôle interne.

9/ Renforcer et pérenniser, dès 2016, l'inspection des services de renseignement. Elle pourrait comprendre deux instances, la première permanente consacrée à l'audit des procédures de contrôle interne et la seconde, rassemblant des inspecteurs de plusieurs ministères afin d'analyser des sujets plus généraux. Elle serait placée auprès du SGDSN.

II. PROPOSITIONS RELATIVES À LA SURVEILLANCE INTERNATIONALE

10/ Organiser des retours d'expériences réguliers sur les dispositifs collaboratifs et coopératifs mis en place par les services, pour en améliorer le fonctionnement et, à terme, servir de base à une réflexion sur une éventuelle réorganisation. L'organisation du recueil de ces retours d'expérience pourrait être confiée au CNR, en s'appuyant au besoin sur la définition d'une méthodologie d'évaluation préparée par l'inspection des services de renseignement.

11/ Procéder à ***

12/ Procéder à ***

13/ Mettre en place un dispositif d'évaluation *** et inclure ces indicateurs dans le rapport d'activité des services qui est transmis chaque année à la DPR.

14/ Demander au CNR de s'assurer, *** et qu'au besoin, il soit en mesure de réaliser les arbitrages nécessaires.

15/ S'assurer de ***

16/ Demander au CNR ***

17/ Amplifier les efforts entrepris pour conforter les moyens du renseignement humain.

18/ Définir dans les meilleurs délais par le moyen d'une instruction générale du Premier ministre, le cadre formel de présentation des demandes d'autorisation dans le respect des exigences posées par le législateur dans la loi du 27 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

19/ Compte tenu de la nature de la menace, la mise en place de façon pragmatique d'un travail collaboratif entre les services est indispensable tant pour déjouer ou entraver les actions terroristes sur le territoire national que pour affaiblir les capacités de Daech au plus loin.

Définir la place du CNR dans le suivi et l'évaluation du fonctionnement des dispositifs de travail collaboratif entre les services, notamment dans le cadre de la lutte contre le terrorisme

Approfondir cette coopération pour améliorer l'accès aux informations et fluidifier certaines procédures.

20/ Saisir toutes les opportunités pour faire progresser la coopération européenne dans le cadre de la lutte contre le terrorisme, inciter nos partenaires et les instances européennes à mieux renseigner le fichier SIS, à améliorer le code frontière Schengen notamment son article 7 et à examiner le renforcement de l'efficacité des contrôles aux frontières extérieures de l'espace Schengen au premier trimestre 2016.

21/ Accélérer la montée en charge du système SETRADER, en lien avec le déploiement du PNR.

22/ Inscrire à l'ordre du jour du Parlement, le projet de loi de transposition de la directive PNR dans les trois mois suivant son adoption et mettre en œuvre sans délai le projet de PNR national.

23/ Poursuivre dans la durée l'effort de montée en puissance des services de renseignement par l'affectation de moyens supplémentaires et non par redéploiement interne

III. PROPOSITIONS RELATIVES À L'ÉVALUATION DE LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT

24/ Remettre le rapport annuel de synthèse des crédits au printemps de l'année N+1.

25/ Faire figurer des indicateurs de performance dans le rapport de synthèse des crédits.

26/ Nommer un chef de service à la tête l'inspection des services de renseignement.

27/ Donner à la DPR la capacité de saisir l'inspection des services de renseignement de thèmes d'études.

28/ Communiquer le rapport annuel d'activité des services de renseignement à la DPR au cours du premier semestre de l'année N+1.

29/ Élaborer et diffuser un rapport public élaboré par le CNR, afin de mieux faire connaître l'activité des services de renseignement et de développer la culture du renseignement.

ANNEXE 1



Délégation parlementaire au renseignement

COMMUNIQUE DE PRESSE

le 26 novembre 2015

Après les tragiques attentats du 13 novembre, la délégation parlementaire au renseignement a entendu, ensemble, le directeur général de la sécurité extérieure et le directeur général de la sécurité intérieure.

Elle a pris connaissance de l'évolution des menaces terroristes dont l'intensité reste à un niveau très élevé. La délégation estime qu'avec les attentats du 13 novembre, une nouvelle étape a été franchie dans l'échelle des risques.

Elle a pu apprécier le degré maximal de mobilisation des services, qui concentrent leurs moyens et leurs compétences pour prévenir et déjouer, autant que faire se peut, de nouvelles attaques, et prendre connaissance de l'adaptation des dispositifs mis en œuvre.

La réponse de sécurité et de défense est adaptée à court terme, mais la mise en œuvre de certaines capacités (recrutements, formation, intégration, déploiement de nouveaux moyens) demandera du temps.

Elle ne sera efficace que si, parallèlement, sont engagés les efforts diplomatiques nécessaires pour trouver une solution politique en Syrie et en Irak et, sur le territoire national, sont apportées des réponses pertinentes aux situations de désespoir qui conduisent certains jeunes vers l'islamisme radical.

Dans cette période difficile et face à cette menace, la délégation appelle les Français à faire preuve de vigilance et d'attention, afin de faciliter l'action des services de l'État.

Face aux incertitudes de la situation, la délégation recommande à tous ceux qui ont à s'exprimer sur ces sujets de faire preuve de la plus grande responsabilité.

La délégation parlementaire au renseignement exerce le contrôle parlementaire de l'action du Gouvernement en matière de renseignement et évalue la politique publique en ce domaine

Assistaient à cette réunion : M. Jean-Pierre RAFFARIN, , président de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, président de la Délégation parlementaire au renseignement ; M. Philippe BAS, président de la commission des Lois du Sénat ; M. Jean-Jacques URVOAS, , président de la commission des Lois de l'Assemblée nationale ; MM. Michel BOUTANT et François-Noël BUFFET, sénateurs , MM Jacques MYARD, et M. Philippe NAUCHE. députés

ANNEXE 2

Les recommandations formulées par la délégation depuis 2012

Rapport 2012

Proposition n° 1 : Renforcer les liaisons entre tous les échelons du renseignement intérieur.

Proposition n° 2 : Renforcer sensiblement les moyens de lutte contre le terrorisme.

Proposition n° 3 : Se doter des moyens permettant de suivre les déplacements de personnes par voie aérienne vers des destinations sensibles, y compris lorsque les trajets comportent une ou des escales.

Proposition n° 4 : Aborder la question du positionnement de la DRPP par rapport aux autres services de renseignement.

Proposition n° 5 : Veiller à la bonne articulation entre les services départementaux d'information générale et le renseignement intérieur.

Proposition n° 6 : Stabiliser les effectifs de la DPSD et de la DRM à leur niveau actuel.

Proposition n° 7 : Poursuivre le renforcement des effectifs de la DGSE, de Tracfin et de la DNRED, ainsi que ceux de la DCRI (devenue DGSI).

Proposition n° 8 : Diversifier le recrutement de la DCRI en lui permettant notamment de recruter des contractuels, linguistes ou spécialistes de haut niveau, ce qui nécessite de lui accorder une véritable autonomie de gestion.

Proposition n° 9 : Poursuivre la modernisation de la gestion des ressources humaines, la diversification du recrutement et l'amélioration de la mobilité entre les services.

Proposition n° 10 : Confirmer et amplifier les capacités de renseignement mises en œuvre par les armées, en particulier concernant le lancement du programme de satellite d'écoute électromagnétique CERES, la composante optique du système de satellite d'observation spatiale MUSIS, l'acquisition de drones MALE équipés de capacités optiques et électromagnétiques et l'amplification des programmes de renseignement électromagnétique lancés depuis 2008.

Proposition n° 11 : Accentuer la mutualisation des capacités, en renforçant notamment le rôle du coordonnateur national du renseignement, en renforçant les capacités exploitées par la DGSE au profit de la communauté du renseignement et en consolidant l'accès des autres services aux capacités mutualisées de la DGSE.

Proposition n° 12 : Garantir que les investissements nécessaires au renforcement des capacités techniques des services de renseignement fassent l'objet d'une priorité et d'un suivi effectif et régulier, sous le contrôle du Premier ministre, lors du vote du budget et de son exécution.

Proposition n° 13 : Faire de la protection et de la défense des systèmes d'information, en particulier de l'État, des entreprises publiques ou privées de secteurs stratégiques et des infrastructures d'importance vitale (énergie, transport, santé, etc.) une priorité de notre politique de défense et de sécurité nationale.

Proposition n° 14 : Poursuivre le renforcement des moyens et des effectifs de l'ANSSI dans les prochaines années, de même que ceux affectés à cette tâche au sein des services de renseignement.

Proposition n° 15 : Introduire une obligation de déclaration en cas d'incident ou d'attaque informatique significative qui s'appliquerait aux entreprises et aux opérateurs d'importance vitale, afin que l'État puisse être réellement informé de ces attaques.

Proposition n° 16 : Doter notre pays, au-delà des capacités de cyberdéfense, de capacités offensives, tant dans les services spécialisés que dans les armées.

Proposition n° 17 : Unifier les dispositifs en matière d'interception des télécommunications prévus d'un côté par la loi du 10 juillet 1991 (article L. 244-2 de code de la sécurité intérieure), de l'autre par la loi du 23 janvier 2006 (dispositions récemment prorogées jusqu'en 2015) en répondant aux besoins des services tout en sécurisant le cadre juridique.

Proposition n° 18 : Simplifier le dispositif législatif existant en harmonisant les dispositions relatives aux prérogatives des différents services, quel que soit leur ministère de rattachement (en particulier défense et intérieur), et aux finalités qui leur permettent d'agir (terrorisme, intérêts fondamentaux de la Nation).

Rapport 2013

Proposition n° 1 : Mettre à profit l'autonomie nouvelle de la DGSI pour dynamiser la gestion de ses ressources humaines et procéder au recrutement des spécialistes de haut niveau dont elle a impérativement besoin.

Proposition n° 2 : Reconstruire une chaîne hiérarchique permettant d'animer et d'assurer la reconnaissance de la filière du renseignement territorial.

Proposition n° 3 : Garantir que le rattachement du renseignement territorial à la sécurité publique ne nuise pas aux nécessaires relations qu'il devra entretenir avec d'autres services.

Proposition n° 4 : Formaliser les liens tissés entre la DRPP et la DCRI à l'occasion de la création de la DGSI.

Proposition n° 5 : Garantir une étroite coordination entre le SCRT et la DRPP.

Proposition n° 6 : Exclure les différents programmes (ou actions et sous-action) budgétaires relatifs aux services de renseignement du mécanisme dit de la « réserve de précaution » par une directive adressée aux différents gestionnaires de programmes budgétaires afin de tenir compte du caractère prioritaire de leur action et de ne pas risquer de fragiliser, dès le début de l'année, les moyens dont disposent les services de renseignement.

Proposition n° 7 : Garantir la bonne mise en œuvre des mesures inscrites dans la loi de programmation militaire concernant le recrutement d'effectifs supplémentaires au sein de la DGSI, de la DGSE et de la DRM et de la DPSD et concernant le lancement de programmes capacitaires, en particulier les programmes satellitaires MUSIS et CERES et l'acquisition ainsi que la modernisation de drones MALE et tactiques.

Proposition n° 8 : Renforcer la diversification du recrutement des services et en particulier de la DGSI, avec notamment le recrutement des personnels spécialisés évoqués ci-dessus.

Proposition n° 9 : Poursuivre et accentuer le renforcement des moyens humains et techniques consacrés à la cyberdéfense, au sein de l'ANSSI, des armées, de la DGA et des services spécialisés et insiste sur la nécessité que le renseignement en matière de cyberdéfense constitue une forte priorité.

Rapport 2014

Proposition n° I-1 : Rattacher le coordonnateur national du renseignement à la fois au Président de la République et au Premier ministre ;

Proposition n° I-2 : Offrir la possibilité à la DPR d'auditionner, au-delà des directeurs des services, les directeurs d'administration centrale œuvrant au sein des services de renseignement dont les postes sont pourvus en conseil des ministres ou publiés au Journal officiel ;

Proposition n° I-3 : Réfléchir à la présence des membres de droit au sein de la DPR ;

Proposition n° I-4 : Établir une communauté du renseignement à plusieurs cercles concentriques.

Proposition n° II-1 : Mettre en place le système PNR à l'échelon national dans les plus brefs délais et promouvoir sa survenance à l'échelle européenne ;

Proposition n° II-2 : Mener une réflexion concernant l'amélioration du système SETRADER ;

Proposition n° II-3 : Initier une amélioration du code frontières Schengen et notamment de son article 7.

Proposition n° III-1 : Adopter une législation relative à la protection du secret des affaires ;

Proposition n° III-2 : Élever les peines d'amende aux articles 323-1 à 3 du code pénal afin de réprimer l'espionnage informatique ;

Proposition n° III-3 : Assurer une meilleure prise en charge de la grande criminalité organisée et de la grande délinquance financière internationales par les services de renseignement ;

Proposition n° III-4 : Octroyer près de 50 ETPT supplémentaires à Tracfin ;

Proposition n° III-5 : Accroître les liens entre la DGSI et Tracfin, notamment par la désignation d'un référent au sein du premier service ;

Proposition n° III-6 : Modifier l'article 40 du CPP afin de protéger les renseignements provenant de services étrangers ainsi que l'identité des agents, sources et collaborateurs des services de renseignement ;

Proposition n° III-7 : Octroyer à Tracfin la possibilité d'agir d'initiative ;

Proposition n° III-8 : Octroyer la possibilité à Tracfin d'enquêter sur des mouvements financiers légaux ;

Proposition n° III-9 : Maintenir et valoriser les capacités de la DNRED ;

Proposition n° III-10 : Développer la mission de la DGSI de lutte contre les organisations criminelles internationales susceptibles d'affecter la sécurité nationale ;

Proposition n° III-11 : Définir précisément les axes de recherche et de collecte du REF pour la DGSE ;

Proposition n° III-12 : Établir des relations pérennes entre la DPSD et Bercy ;

Proposition n° III-13 : Mettre en place une sensibilisation aux questions de sécurité et de renseignement prise en charge par l'Institut de la gestion publique et du développement économique (IGPDE) en partenariat avec l'Académie du renseignement ;

Proposition n° III-14 : Créer une instance de coordination du REF au sein de Bercy afin de produire une doctrine adaptée et accroître les relations avec les différents services de renseignement ;

Proposition n° III-15 : Désigner un référent REF par service de renseignement (à la DGSI, il pourrait s'agir de la même personne que celle visée par la proposition n° 5) ;

Proposition n° III-16 : Déterminer une politique d'influence européenne ;

Proposition n° III-17 : Créer un comité interministériel placé auprès du Premier ministre afin de déterminer les critères d'éligibilité pour aider des entreprises privées dans le domaine du REF ou attribuer cette mission à la D2IE ;

Proposition n° III-18 : Organiser, au sein des services de renseignement, le traitement de l'information ouverte en matière de REF ;

Proposition n° III-19 : Maintenir le SCIE auprès du secrétaire général de Bercy ;

Proposition n° III-20 : Nommer le chef du SCIE adjoint du D2IE ;

Proposition n° III-21 : Créer une direction de l'information économique et financière à Bercy construite autour de Tracfin ;

Proposition n° III-22 : Maintenir les efforts accomplis en faveur d'un dispositif public d'intelligence économique efficace, coordonné et en prise avec le REF.

Proposition n° IV-1 : Protéger, dans le droit français, l'activité des agents de la DGSE à l'étranger ;

Proposition n° IV-2 : Prévoir un mécanisme de dispense de publication des délégations de signature ;

Proposition n° IV-3 : Systématiser les poursuites à l'encontre des personnes dévoilant l'identité d'agents des services de renseignement ;

Proposition n° IV-4 : Inscrire dans la loi les missions des services de renseignement avec précision ;

Proposition n° IV-5 : Développer le contrôle interne administratif ;

Proposition n° IV-6 : Créer la fonction de chef de l'inspection des services de renseignement ;

Proposition n° IV-7 : Réaffirmer le principe de centralisation de la mise en œuvre des techniques de recueil du renseignement par le biais du GIC ;

Proposition n° IV-8 : Confier à une AAI (sur le modèle de la CNCIS) le soin de délivrer un avis et de contrôler la mise en œuvre des techniques de recueil du renseignement ;

Proposition n° IV-9 : Accroître considérablement les moyens humains, techniques et budgétaires de la CNCIS et, in fine, de la future AAI ;

Proposition n° IV-10 : Accroître le nombre de membres de la CNCIS et, in fine, de la future AAI ;

Proposition n° IV-11 : Remplacer les membres parlementaires par des personnalités qualifiées désignées par le président de chaque Chambre sur proposition de la Délégation parlementaire au renseignement ;

Proposition n° IV-12 : Laisser le soin aux grands corps de désigner les membres de l'AAI et non au pouvoir exécutif (modèle CNIL) ;

Proposition n° IV-13 : Accroître le quota des interceptions de sécurité ;

Proposition n° IV-14 : Conditionner l'application de l'article L. 246-1 du CSI au respect de l'article 226-15 du code pénal relatif au secret des correspondances ;

Proposition n° IV-15 : Supprimer le dispositif de la personnalité qualifiée au profit d'un élargissement des compétences et prérogatives de la CNCIS ;

Proposition n° IV-16 : Transposer au domaine administratif certaines techniques spéciales de police judiciaire ;

Proposition n° IV-17 : Permettre l'interconnexion des fichiers sous certaines conditions très strictes ;

Proposition n° IV-18 : Confier le contrôle des fichiers des services de renseignement à l'AAI chargée de contrôler la mise en œuvre des techniques de recueil du renseignement ;

Proposition n° IV-19 : Confier à l'ISR des missions annuelles de contrôle des fichiers de souveraineté ;

Proposition n° IV-20 : Apporter une définition juridique à la notion d'opérations ;

Proposition n° IV-21 : Mettre en place des voies de recours pour les citoyens par l'intermédiaire de l'AAI chargée de contrôler la mise en œuvre des techniques de recueil du renseignement ;

Proposition n° IV-22 : Donner la capacité à l'AAI chargée de contrôler la mise en œuvre des techniques de recueil du renseignement de délivrer un avis consultatif de légalité concernant ces techniques dans le cadre d'un contentieux judiciaire.

Proposition n° V-1 : Dans le rapport annuel de synthèse exhaustif des crédits consacrés au renseignement, présenter des prévisions d'exécution des emplois pour l'année en cours ;

Proposition n° V-2 : Dans le rapport annuel de synthèse exhaustif des crédits consacrés au renseignement, présenter des prévisions de dépenses des crédits de paiement pour l'année en cours ;

Proposition n° V-3 : Étendre l'application des articles L. 4221-3, L. 4241-1 et 3 du code de la défense (réserve opérationnelle et réserve citoyenne) à la DRM ainsi qu'à la DPSD ;

Proposition n° V-4 : Aménager les règles d'affectation à la DRM afin de bénéficier de durées plus longues ;

Proposition n° V-5 : Permettre à la DRM de recruter ses personnels dans le vivier des officiers et sous-officiers de chacune des armées ;

Proposition n° V-6 : Permettre aux militaires de postuler directement à la DRM ;

Proposition n° V-7 : Permettre à la DRM d'accroître sa capacité de recrutement sur contrats ;

Proposition n° V-8 : Nouer des collaborations plus étroites avec des experts civils de divers horizons ;

Proposition n° V-9 : Désigner des civils pour exercer des responsabilités au sein de la DRM ;

Proposition n° V-10 : Créer un second poste de directeur adjoint de la DRM confié à un civil ;

Proposition n° V-11 : Mettre en œuvre les conditions d'une réelle mobilité interservices ;

Proposition n° V-12 : Accroître les effectifs de la DPSD ;

Proposition n° V-13 : Accroître le nombre de civils à la DPSD ;

Proposition n° V-14 : Appliquer les propositions n° 2, 3, 4, 5, 6, 7 et 9 à la DPSD ;

Proposition n° V-15 : Créer un statut d'emploi transfonction publique d'experts renseignement communs aux six services ;

Proposition n° V-16 : Offrir des garanties statutaires aux membres des services de renseignement sur le modèle de celles offertes aux agents de la DGSE ;

Proposition n° V-17 : Mettre en œuvre une réflexion juridique et budgétaire sur le recours aux contractuels dans les services de renseignement ;

Proposition n° V-18 : Considérer que le retrait d'habilitation constitue une clause de rupture de contrat et créer des voies de recours effectives ;

Proposition n° V-19 : Doter les services de référents juridiques ;

Proposition n° V-20 : Encourager le financement de recherches doctorales par les services de renseignement ;

Proposition n° V-21 : Promouvoir l'inscription de thématiques de recherche propres aux services de renseignement dans les appels à projets lancés par l'Agence nationale de la recherche (ANR) ;

Proposition n° V-22 : Signer des conventions avec des écoles doctorales dans le domaine du renseignement ;

Proposition n° V-23 : Créer une revue scientifique dédiée au domaine du renseignement ;

Proposition n° V-24 : Instaurer un comité scientifique consultatif à l'Académie du renseignement ;

Proposition n° V-25 : Offrir la capacité de rémunérer des études confiées à des spécialistes en réponse à une commande des services de renseignement ;

Proposition n° V-26 : Développer une réserve opérationnelle ou citoyenne propre aux services de renseignement.

Proposition n° VI-1 : Rationaliser l'implantation territoriale de la DGSI ;

Proposition n° VI-2 : Résoudre le problème immobilier induit par les recrutements réalisés par la DGSI ;

Proposition n° VI-3 : Préserver les effectifs dédiés au contre-espionnage et à la sécurité économique à la DGSI ;

Proposition n° VI-4 : Ne pas favoriser la judiciarisation du renseignement produit par le SCRT ;

Proposition n° VI-5 : Assurer un surcroît de moyens humains et techniques au SCRT pour la prise en charge de la surveillance d'éléments radicaux ;

Proposition n° VI-6 : Étoffer la coopération opérationnelle entre le SCRT et la Gendarmerie sans recourir à des nominations croisées ;

Proposition n° VI-7 : Désigner des DDSP adjoint en charge du renseignement dans les départements ;

Proposition n° VI-8 : Modifier les arrêtés de nomination délivrés pour le SCRT ;

Proposition n° VI-9 : Attribuer des personnels administratifs en nombre suffisant au SCRT et le doter d'arrêtés de nomination ;

Proposition n° VI-10 : Créer dans des délais restreints un certificat d'analyste de renseignement territorial ;

Proposition n° VI-11 : Mettre en place un plan et des équipes de formation pour le SCRT ;

Proposition n° VI-12 : Mutualiser les formations entre le SCRT et la SDAO sur les points de convergence ;

Proposition n° VI-13 : Ouvrir l'Académie du renseignement aux personnels du SCRT ;

Proposition n° VI-14 : Diminuer les contraintes de mobilité pour les personnels affectés au SCRT ;

Proposition n° VI-15 : Résoudre le problème immobilier induit par les recrutements réalisés par le SCRT ;

Proposition n° VI-16 : Octroyer au SCRT un accès intégral au TAJ ;

Proposition n° VI-17 : Réfléchir au cadre juridique des activités du SCRT (moyens techniques et protection des agents) ;

Proposition n° VI-18 : Réfléchir au cadre juridique des activités de la SDAO (moyens techniques et protection des agents) ;

Proposition n° VI-19 : Revaloriser les moyens techniques et budgétaires alloués à la DRPP ;

Proposition n° VI-20 : Céder à la DCPAF la mission de lutte contre l'immigration clandestine assumée par la DRPP ;

Proposition n° VI-21 : Consacrer des moyens humains plus importants au renseignement pénitentiaire au niveau central et dans les établissements ;

Proposition n° VI-22 : Réfléchir au cadre juridique des activités du bureau du renseignement pénitentiaire (BRP) (moyens techniques et protection des agents) ;

Proposition n° VI-23 : Ouvrir l'Académie du renseignement aux personnels du BRP ;

Proposition n° VI-24 : Étoffer la collaboration entre le BRP et les services compétents dans le domaine du renseignement intérieur.

Proposition n° VII-1 : Étudier les conditions dans lesquelles la future AAI, chargée de contrôler les techniques du renseignement, pourrait être informée des interceptions de sécurité opérées à l'étranger.

Proposition n° VII-2 : Consolider la souveraineté de notre pays en matière d'autonomie stratégique dans le domaine du renseignement d'origine électromagnétique.

Proposition n° VII-3 : Explorer les conditions d'un partenariat dans un cadre européen.

ANNEXE 3

**LA MISE EN ŒUVRE DES PROPOSITIONS FORMULÉES PAR
LA DPR DANS SON RAPPORT 2014**

**I. RÉPONSES AU QUESTIONNAIRE ADRESSÉ AU
COORDONNATEUR NATIONAL DU RENSEIGNEMENT**

**II. RÉPONSES AU QUESTIONNAIRE ADRESSÉ AU MINISTRE
DES FINANCES ET DES COMPTES PUBLIC**

ANNEXE 4

Annonces du Premier ministre du 21 janvier 2015 (*source : CNR - Rapport annuel de synthèse exhaustif des crédits consacrés au renseignement - exercice 2014*)

A la suite des événements des 9 et 11 janvier 2015, le Premier ministre a annoncé le 21 janvier une série de mesures visant à renforcer la lutte contre le terrorisme.

Au total, entre 2015 et 2018, la création de 2 680 emplois a été annoncée :

- 1 400 pour le ministère de l'intérieur, dont 500 pour la DGSI, 500 pour les services de renseignement territorial et 100 pour la direction du renseignement de la préfecture de police de Paris ;

- 950 pour le ministère de la justice ;

- 250 pour le ministère de la défense ;

- 80 pour le ministère des finances, et des comptes publics, dont 70 au bénéfice de la direction générale des douanes et droits indirects.

En outre, 425 M€ de crédits d'investissement, d'équipement et de fonctionnement seront consacrés à la lutte contre le terrorisme, au cours des 3 prochaines années, dont 233 M€ pour le ministère de l'Intérieur et 181 M€ pour celui de la Justice.

Le tableau ci-dessous récapitule les renforcements annoncés, s'agissant des services présentés dans le présent rapport.

ANNEXE 5

Lettre adressée à l'Inspection des services de renseignement sur le contenu et la forme du rapport d'activité des services



Délégation parlementaire au renseignement

M***

75*** PARIS

Le 16 juillet 2015

M***,

Lors de notre entretien du 22 juin dernier, nous étions convenus que j'informerai la délégation parlementaire au renseignement des travaux que conduit actuellement l'Inspection générale des services de renseignement en vue de la préparation du rapport d'activité des services qui doit, aux termes des dispositions du 3° du I de l'article 6 nonies de l'ordonnance n°1100 du 17 novembre 1958, être communiqué chaque année à ladite délégation.

Au cours de la réunion de la délégation, le 16 juillet, j'ai pu recueillir le point de vue des membres sur ce que devrait contenir ce rapport et sur la forme qu'il pourrait revêtir.

CONTENU DU RAPPORT

1. Un rappel des missions des services telles qu'elles sont prévues par la loi et les règlements ainsi qu'un rappel des objectifs fixés par la stratégie nationale du renseignement et par le plan national d'orientation du renseignement. Une présentation des objectifs nouveaux assignés aux services, par rapport à ces textes cadres pour l'année concernée (issus des conseils du renseignement ou des conseils de défense).
2. Une présentation de l'activité de chacun des services faisant apparaître leur contribution à la politique publique du renseignement telle que définie par les textes susvisés (1.). La présentation s'efforcera de mettre en exergue les productions concrètes des services à partir d'outils statistiques (indicateurs d'activité) qui pourraient être issus de leurs tableaux de bord internes et en établissant des comparaisons avec les exercices antérieurs (et avec les objectifs

assignés, s'ils existent). Elle pourra être illustrée par des cas concrets à l'image des cas typologiques présentés dans le rapport d'activité de TRACFIN.

3. Une présentation des moyens (budgétaires, humains, matériels) comprenant des éléments statistiques avec des comparaisons avec les exercices antérieurs (et les prévisions si elles existent), des indicateurs de gestion issus des tableaux de bord internes. Une présentation des politiques RH de recrutement, de déroulement de carrière et de formation des personnels (éléments qui pourraient figurer dans le bilan social d'une entreprise). Une présentation des politiques d'investissements (acquisition, recherche).
4. Une présentation transversale de la coordination entre les services à travers une description des modes de coopération institués ou occasionnels et des éléments statistiques. Un développement sur le rôle et l'activité du CNR.
5. Une présentation des activités de coopération internationale.

FORME DU RAPPORT

La forme doit être exhaustive.

Le document doit être conçu en priorité comme un outil pour permettre à la DPR d'assurer sa mission de contrôle de l'action du gouvernement et d'évaluation de la politique publique du renseignement.

Le document doit faire apparaître explicitement les éléments couverts par le secret de la défense nationale et ceux qui ne le sont pas.

Si une version doit être rendue publique, dans une perspective de transparence et de développement de la culture du renseignement, cela ne pourra être qu'une synthèse de ce document.

Le document doit être annuel et les données et outils statistiques mis en place sont conçus pour permettre la constitution de séries et de comparaisons d'un exercice à l'autre.

Je vous remercie pour l'attention que vous pourrez porter à ces recommandations et vous prie de croire, M ***, à ma parfaite considération.

Le Président
Jean-Pierre RAFFARIN

ANNEXE 6

Services du deuxième cercle autorisés à recourir à certaines techniques de renseignement

<u>Direction générale de la police nationale (DGPN)</u>
Unité de coordination de la lutte anti-terroriste (UCLAT)
Service central des courses et jeux (DCPJ)
Sous-direction de la lutte contre la criminalité organisée et la délinquance financière (DCPJ)
Sous-direction anti-terroriste (DCPJ)
Sous-direction de la lutte contre la cybercriminalité (DCPJ)
Directions régionales et interrégionales de police judiciaire (DCPJ)
Services régionaux de police judiciaire (DCPJ)
Antennes de police judiciaire (DCPJ)
Unités en charge de la police judiciaire des directions déconcentrées de la PAF (DCPAF)
Directions de la police aux frontières d'Orly et de Roissy (DCPAF)
Brigades mobiles de recherche zonales (DCPAF)
L'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (OCRIEST) (DCPAF)
L'unité judiciaire du service national de la police ferroviaire (DCPAF)
Service central du renseignement territorial et services départementaux du renseignement territorial (DCSP)
Suretés départementales (DCSP)

<u>Direction générale de la gendarmerie nationale (DGGN)</u>
Sous-direction de l'anticipation opérationnelle (SDAO)
Sous-direction de la police judiciaire
Sections de recherche de la gendarmerie nationale
<u>Préfet de police de Paris</u>
Sous-direction de la sécurité intérieure (Direction du renseignement de la préfecture de police de Paris (DRPP))
Sous-direction du renseignement territorial (DRPP)
Sous-direction des brigades centrales (Direction régionale de la police judiciaire)
Sous-direction des affaires économiques et financières (Direction régionale de la police judiciaire)
Sous-direction des services territoriaux (Direction régionale de la police judiciaire)
Suretés territoriales direction de la sécurité et de la proximité de l'agglomération parisienne (DSPAP)
<u>Sous l'autorité d'emploi du ministère de la défense</u>
Sections de recherche de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement

ANNEXE 7

Récapitulatif par service autorisé et par finalités poursuivies, des techniques ouvertes aux services du second cercle, en application du décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure

Service concerné	Finalités poursuivies	Techniques autorisées
Direction générale de la police nationale (DGPN)		
Unité de coordination de la lutte anti-terroriste (UCLAT)	4° La prévention du terrorisme 5° La prévention a) Des atteintes à la forme républicaine des institutions ; b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;	- accès administratif aux données de connexion (L. 851-1) ;
Service central des courses et jeux (DCPJ)	6° La prévention de la criminalité et de la délinquance organisées	- accès administratif aux données de connexion (L. 851-1) - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Sous-direction de la lutte contre la criminalité organisée et la délinquance financière (DCPJ)	6° La prévention de la criminalité et de la délinquance organisées	- accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ;

Service concerné	Finalités poursuivies	Techniques autorisées
		<ul style="list-style-type: none"> - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I); - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Sous-direction anti-terroriste (DCPJ)	4° La prévention du terrorisme	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I); - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer,

Service concerné	Finalités poursuivies	Techniques autorisées
		<p>de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <ul style="list-style-type: none"> - mise en place, utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1) et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu d'habitation pour la seule finalité de prévention du terrorisme - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme.
Sous-direction de la lutte contre la cybercriminalité (DCPJ)	<p>4° La prévention du terrorisme 6° La prévention de la criminalité et de la délinquance organisées</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ;

Service concerné	Finalités poursuivies	Techniques autorisées
		<ul style="list-style-type: none"> - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme.
<p>Directions régionales et interrégionales de police judiciaire (DCPJ) (11 directions)</p>	<p>4° La prévention du terrorisme 6° La prévention de la criminalité et de la délinquance organisées</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une

Service concerné	Finalités poursuivies	Techniques autorisées
		balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Services régionaux de police judiciaire (DCPJ) (8 services)	4° La prévention du terrorisme 6° La prévention de la criminalité et de la délinquance organisées	- accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Antennes de police judiciaire (DCPJ)	4° La prévention du terrorisme 6° La prévention de la criminalité et de la délinquance organisées	- accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)

Service concerné	Finalités poursuivies	Techniques autorisées
Unités en charge de la police judiciaire des directions déconcentrées de la PAF (DCPAF)	6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - Interception de sécurité (L. 852-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Directions de la police aux frontières d'Orly et de Roissy (DCPAF)	6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - Interception de sécurité (L. 852-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Brigades mobiles de recherche zonales (DCPAF)	6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - Interception de sécurité (L. 852-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
L'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (OCRIEST) (DCPAF)	6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un

Service concerné	Finalités poursuivies	Techniques autorisées
		<p>lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <ul style="list-style-type: none"> - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;
L'unité judiciaire du service national de la police ferroviaire (DCPAF)	6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - Interception de sécurité (L. 852-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Services du renseignement territorial (DCSP)	<p>1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;</p> <p>4° La prévention du terrorisme ;</p> <p>5° La prévention :</p> <p>a) Des atteintes à la forme républicaine des institutions ;</p> <p>b) Des actions tendant au maintien ou à la</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) : pour l'unité nationale et les unités territoriales de recherche et d'appui des services du renseignement territorial ; - Interception de sécurité (L. 852-1 I) ; - Interception de correspondances par le biais d'un IMSI catcher (L. 852-1 II) : pour l'unité nationale et les unités territoriales de

Service concerné	Finalités poursuivies	Techniques autorisées
	<p>reconstitution de groupements dissous en application de l'article L. 212-1 ;</p> <p>c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;</p> <p>6° La prévention de la criminalité et de la délinquance organisées</p>	<p>recherche et d'appui des services du renseignement territorial ;</p> <ul style="list-style-type: none"> - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) : pour l'unité nationale et les unités territoriales de recherche et d'appui des services du renseignement territorial ; - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) : pour l'unité nationale et les unités territoriales de recherche et d'appui des services du renseignement territorial ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) : pour l'unité nationale et les unités territoriales de recherche et d'appui des services du renseignement territorial ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) : pour l'unité nationale et les unités territoriales de recherche et d'appui des services du renseignement territorial ; - mise en place, utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1)

Service concerné	Finalités poursuivies	Techniques autorisées
		<p>et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu d'habitation pour la seule finalité de prévention du terrorisme : pour l'unité nationale de recherche et d'appui du service central du renseignement territorial ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme.</p> <p>: pour l'unité nationale de recherche et d'appui du service central du renseignement territorial ;</p>
Sûretés départementales (DCSP)	6° La prévention de la criminalité et de la délinquance organisées	<p>- accès administratif aux données de connexion (L. 851-1) ;</p> <p>- localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ;</p> <p>- balises (L. 851-5) ;</p> <p>- Interception de sécurité (L. 852-1 I) ;</p> <p>- mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) : pour l'unité nationale de recherche et d'appui du service central du renseignement territorial ;</p>
Direction générale de la gendarmerie nationale (DGGN)		
SDAO (DOE)	<p>1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;</p> <p>4° La prévention du terrorisme ;</p> <p>5° La prévention :</p> <p>a) Des atteintes à la forme républicaine des institutions ;</p> <p>b) Des actions tendant au maintien ou à la reconstitution de</p>	<p>- accès administratif aux données de connexion (L. 851-1) ;</p> <p>- localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ;</p> <p>- balises (L. 851-5) ;</p> <p>- IMSI catcher (L. 851-6) ;</p> <p>- Interception de sécurité (L. 852-1 I) ;</p> <p>- Interception de correspondances par le biais d'un IMSI catcher (L. 852-1 II) ;</p> <p>- utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ;</p>

Service concerné	Finalités poursuivies	Techniques autorisées
	<p>groupements dissous en application de l'article L. 212-1 ;</p> <p>c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;</p>	<p>- utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ;</p> <p>- mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1) et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu d'habitation pour la seule finalité de prévention du terrorisme ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I</p>

Service concerné	Finalités poursuivies	Techniques autorisées
		1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme.
Sous-direction de la police judiciaire (DOE)	1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 4° La prévention du terrorisme ; 6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1) et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu

Service concerné	Finalités poursuivies	Techniques autorisées
		<p>d'habitation pour la seule finalité de prévention du terrorisme</p> <ul style="list-style-type: none"> - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme
<p>Sections de recherche de la gendarmerie nationale</p>	<p>4° La prévention du terrorisme ; 6° La prévention de la criminalité et de la délinquance organisées</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) :
Préfet de police de Paris		
<p>Sous-direction de la sécurité intérieure (DRPP)</p>	<p>1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 4° La prévention du terrorisme ; 5° La prévention : a) Des atteintes à la forme républicaine des</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - Interception de correspondances par le biais d'un IMSI catcher (L. 852-1 II) ; - utilisation de dispositifs techniques

Service concerné	Finalités poursuivies	Techniques autorisées
	<p>institutions ;</p> <p>b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;</p> <p>c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;</p> <p>6° La prévention de la criminalité et de la délinquance organisées</p>	<p>permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ;</p> <p>- utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ;</p> <p>- mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3);</p> <p>- mise en place, utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1) et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu d'habitation pour la seule finalité de prévention du terrorisme ;</p> <p>- mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ;</p> <p>- mise en place, utilisation ou retrait d'un</p>

Service concerné	Finalités poursuivies	Techniques autorisées
		dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme
Sous-direction du renseignement territorial (DRPP)	<p>1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;</p> <p>4° La prévention du terrorisme ;</p> <p>5° La prévention :</p> <p>a) Des atteintes à la forme républicaine des institutions ;</p> <p>b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;</p> <p>c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;</p> <p>6° La prévention de la criminalité et de la délinquance organisées</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Sous-direction des brigades centrales	4° <i>La prévention</i>	- accès administratif aux données de connexion (L. 851-1) ;

Service concerné	Finalités poursuivies	Techniques autorisées
<p>(Direction régionale de la police judiciaire)</p>	<p><i>du terrorisme ;</i> 6° La prévention de la criminalité et de la délinquance organisées</p>	<ul style="list-style-type: none"> - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - - Interception de sécurité (L. 852-1 I) ; - Interception de correspondances par le biais d'un IMSI catcher (L. 852-1 II) : pour la seule brigade de recherche et d'intervention et pour la seule finalité de prévention du terrorisme ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) : (*): pour la section anti-terroriste de la brigade criminelle (pour la seule finalité de prévention du terrorisme) ; (*): pour la brigade de la protection des mineurs (pour la seule finalité de prévention de la criminalité et de la délinquance organisées); - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu

Service concerné	Finalités poursuivies	Techniques autorisées
		<p>privé ne constituant pas un lieu d'habitation (L. 853-3): (*): pour la section anti-terroriste de la brigade criminelle (pour la seule finalité de prévention du terrorisme) (*): pour la brigade de la protection des mineurs (pour la seule finalité de prévention de la criminalité et de la délinquance organisées) ; - mise en place, utilisation et retrait d'une balise (L. 851-5), d'un dispositif d'enregistrement sonore ou image (L. 853-1) et d'un dispositif de captation de données informatiques (L. 853-2 I 1°) dans un lieu d'habitation pour la seule finalité de prévention du terrorisme ; (*): pour la section anti-terroriste de la brigade criminelle (*): pour la brigade de recherche et d'intervention (pour les seules balises (L. 851-5) et dispositif de captation sons/images (L. 853-1) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) (*): pour la section anti-terroriste de la brigade criminelle (pour la seule finalité de prévention du terrorisme) (*): pour la brigade de la protection des mineurs (pour la seule finalité de prévention de la criminalité et de la délinquance organisées) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un lieu d'habitation (L. 853-3) pour la seule finalité de prévention du terrorisme (*): pour la section anti-terroriste de la brigade criminelle</p>
<p>Sous-direction des affaires économiques et financières (Direction régionale de la police judiciaire)</p>	<p>6° La prévention de la criminalité et de la délinquance organisées</p>	<p>- accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques</p>

Service concerné	Finalités poursuivies	Techniques autorisées
		<p>permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ;</p> <ul style="list-style-type: none"> - utilisation de dispositifs techniques permettant d'accéder à des données informatiques contenues dans un système informatique, ou telles qu'elles s'affichent, telles qu'elles y sont introduites ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I) : pour la brigade d'enquête sur les fraudes aux technologies de l'information ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent à l'écran, telle qu'elles sont introduites dans un système de traitement automatisé de données par saisie de caractères ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels (L. 853-2 I 2°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3): <p>(*) : pour la brigade d'enquête sur les fraudes aux technologies de l'information ;</p> <ul style="list-style-type: none"> - mise en place, utilisation ou retrait d'un dispositif technique permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre (L. 853-2 I 1°) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) <p>(*) : pour la brigade d'enquête sur les fraudes aux technologies de l'information</p>
<p>Sous-direction des services territoriaux (Direction</p>	<p>4° La prévention du terrorisme ; 6° La prévention de la criminalité et</p>	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ;

Service concerné	Finalités poursuivies	Techniques autorisées
régionale de la police judiciaire)	de la délinquance organisées	<ul style="list-style-type: none"> - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Suretés territoriales (DSPAP)	6° La prévention de la criminalité et de la délinquance organisées	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) - balises (L. 851-5) ; - Interception de correspondances (L. 852-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)
Sous l'autorité d'emploi du ministère de la défense		
Sections de recherche de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement	<ul style="list-style-type: none"> 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 4° La prévention du terrorisme ; 6° La prévention de la criminalité et de la délinquance organisées 	<ul style="list-style-type: none"> - accès administratif aux données de connexion (L. 851-1) ; - localisation en temps réel d'un terminal sur sollicitation du réseau (L. 851-4) ; - balises (L. 851-5) ; - IMSI catcher (L. 851-6) ; - Interception de sécurité (L. 852-1 I) ; - utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (L. 853-1 I) ; - mise en place, utilisation ou retrait d'une balise (L.851-5) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3) ; - mise en place, utilisation ou retrait d'un dispositif technique permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou

Service concerné	Finalités poursuivies	Techniques autorisées
		confidentiel ou d'images dans un lieu privé (L. 853-1) dans un véhicule ou dans un lieu privé ne constituant pas un lieu d'habitation (L. 853-3)