



N° 1531

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 6 novembre 2013.

AVIS

FAIT

AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION
ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE SUR LE PROJET DE LOI, ADOPTÉ PAR
LE SÉNAT (n° 1473), *relatif à la **programmation militaire** pour les années **2014 à 2019***
et portant diverses dispositions concernant la défense et la sécurité nationale,

PAR M. PATRICE VERCHÈRE
Député

Voir les numéros :

Sénat : 822 (2012-2013), 50, 51, 53, 56 et T.A. 23 (2013-2014).

SOMMAIRE

	Pages
INTRODUCTION	5
AUDITION DE M. ALAIN ZABULON, COORDONNATEUR NATIONAL DU RENSEIGNEMENT	13
AUDITION DE M. PATRICK CALVAR, DIRECTEUR CENTRAL DU RENSEIGNEMENT INTÉRIEUR	25
EXAMEN DES ARTICLES	37
Chapitre I ^{er} bis – Dispositions relatives au contrôle parlementaire de l'exécution de la loi de programmation	37
<i>Article 4 ter</i> : Contrôle sur pièces et sur place pour les membres des commissions parlementaires chargées de la défense	37
<i>Article 4 quater</i> : Réunions de contrôle de l'exécution de la loi de programmation	40
<i>Article 4 quinquies</i> (art. L. 143-5 du code des juridictions financières) : Transmission des observations de la Cour des comptes aux commissions chargées de la défense et des affaires étrangères	40
<i>Article 4 sexies</i> : Rapport et débat au Parlement sur le contrôle de l'exécution des lois de programmation et diverses autres mesures	41
Chapitre II – Dispositions relatives au renseignement	42
<i>Article 5</i> (art. 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958) : Renforcement des prérogatives de la délégation parlementaire au renseignement	42
<i>Article 6</i> (art. 154 de la loi n° 2001-1275 du 28 décembre 2001) : Absorption de la commission de vérification des fonds spéciaux par la délégation parlementaire au renseignement	48
<i>Article 7</i> (art. 656-1 du code de procédure pénale) : Audition d'agents des services de renseignement en dehors des tribunaux et des locaux des services enquêteurs	51
<i>Article 8</i> (art. L. 222-1 du code de la sécurité intérieure) : Élargissement de l'accès des services de renseignement à certains grands fichiers administratifs	53
<i>Article 9</i> (art. L. 232-2 du code de la sécurité intérieure) : Élargissement des finalités d'accès à deux fichiers relatifs aux passagers aériens	54

<i>Article 10</i> (art. L. 232-7 [nouveau] du code de la sécurité intérieure) : Création à titre expérimental d'un nouveau traitement relatif aux données des transporteurs aériens	56
<i>Article 11</i> (art. L. 234-2 du code de la sécurité intérieure) : Accès des services du ministère de la défense aux fichiers de police judiciaire dans le cadre des enquêtes administratives	58
<i>Article 12</i> (art. L. 234-3 du code de la sécurité intérieure) : Accès des services du ministère de la Défense aux fichiers de police judiciaire dans le cadre des enquêtes administratives pour l'exercice de missions ou d'interventions	59
<i>Article 13</i> (art. L. 34-1 et L. 34-1-1 du code des postes et des communications électroniques, art. 6 de la loi n° 2004-575 du 21 juin 2004 et art. L. 222-2, L. 222-3, L. 243-7, L. 245-3, L. 243-12, L. 246-1 à L. 246-5 [nouveaux] du code de sécurité intérieure) : Clarification du cadre juridique relatif à la géolocalisation en temps réel ...	60
Chapitre III – Dispositions relatives à la protection des infrastructures vitales contre la cybermenace	65
<i>Article 14</i> (art. L. 2321-1 et L. 2321-2 [nouveaux] du code de la défense) : Renforcement du dispositif étatique en matière de cyberdéfense	65
<i>Article 15</i> (art. L. 1332-6-1 à L. 1332-6-6 [nouveaux] et L. 1332-7 du code de la défense) : Renforcement des obligations des opérateurs d'importance vitale en matière de sécurité et de défense des systèmes d'information	66
<i>Article 16</i> (art. 226-3 et 226-15 du code pénal) : Extension de la liste des équipements informatiques soumis au régime d'autorisation	68
<i>Article 16 bis</i> (art. L. 2321-3 [nouveau] du code de la défense et L. 336-3 et L. 34-1 du code des postes et des communications électroniques) Accès aux coordonnées des utilisateurs des adresses Internet pour les besoins de la sécurité informatique	69
<i>Article 16 ter</i> (art. 323-3-1 du code pénal et L. 122-6-1 du code de la propriété intellectuelle) : Possibilité d'exercer une activité de recherche ou de développement de produits ou de service de sécurité informatique	69
Chapitre IV – Dispositions relatives au traitement pénal des affaires militaires	70
<i>Article 17</i> (art. L. 211-7 du code de justice militaire) : Régime de présomption en cas de mort violente d'un militaire lors d'une action de combat, à l'occasion d'une opération militaire à l'étranger	70
<i>Article 18</i> (art. 698-2 du code de procédure pénale et L. 211-7 du code de justice militaire) : Mise en mouvement de l'action publique à l'encontre de militaires engagés dans une opération militaire en dehors du territoire français	71
<i>Article 19</i> (art. L. 4123-11 et L. 4123-12 du code de la défense) : Responsabilité pénale des militaires	72
<i>Article 20</i> (art. L. 211-5 et L. 211-22 du code de justice militaire et art. 698-5 du code de procédure pénale) : Correction d'erreurs formelles résultant de la suppression du Tribunal aux armées de Paris et précision sur la procédure applicable aux militaires en temps de paix	73

<i>Article 21</i> (art. 697 du code de procédure pénale) : Spécialisation des juridictions en matière militaire	74
Chapitre V – Dispositions relatives aux ressources humaines.....	74
<i>Section 1 : Dispositions relatives à la protection juridique</i>	74
<i>Article 22</i> : Extension de la protection fonctionnelle aux ayants-droit des militaires décédés en opérations et à certains personnels civils.....	74
PERSONNES ENTENDUES PAR LE RAPPORTEUR POUR AVIS	77

Mesdames, Messieurs,

La commission des Lois s'est saisie pour avis, des articles 4 *ter* à 22 du projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, que le Sénat a adopté le 21 octobre dernier.

Ces 24 articles correspondent à l'ensemble des dispositions relatives au renseignement, au contrôle parlementaire et au cadre juridique dans lequel nos services de renseignement agissent, auquel s'ajoute un article portant sur la protection fonctionnelle des ayants-droit des militaires décédés en opérations et de certains personnels civils.

Depuis la création en 2007 de la délégation parlementaire au renseignement ⁽¹⁾, les pouvoirs publics ont mené une réflexion sur le rôle et les moyens de nos services de renseignement.

Le *Livre blanc sur la défense et la sécurité nationale* de 2008 avait érigé la problématique « connaissance et anticipation », en fonction stratégique, ce qui traduisait la reconnaissance de l'importance du renseignement pour notre sécurité nationale. Ce même Livre blanc constatait : « *Les activités de renseignement ne disposent pas aujourd'hui d'un cadre juridique clair et suffisant. Cette lacune doit être comblée.* » ⁽²⁾

La commission des Lois a ainsi créé, dès le début de la législature, une mission d'information, dont les travaux ont duré neuf mois. Votre rapporteur pour avis, qui était co-rapporteur de cette mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement ⁽³⁾, se félicite que plusieurs des préconisations avancées dans le rapport d'information trouvent une

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

(2) Livre blanc sur la défense et la sécurité nationale, Paris, Odile Jacob/La Documentation française, 2008, p. 142.

(3) MM. Jean-Jacques Urvoas et Patrice Verchère, Pour un « État secret » au service de notre démocratie, rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, doc. AN n° 1022, 14 mai 2013. Votre rapporteur pour avis renvoie à ce rapport pour ce qui est d'une présentation complète de la question du renseignement en France et de son encadrement juridique. Ce document est consultable à l'adresse suivante : <http://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf>

traduction législative dans le présent projet de loi. Il en est ainsi du renforcement des prérogatives de la délégation parlementaire au renseignement, du rapprochement de cette dernière avec la commission de vérification des fonds spéciaux et des différents outils juridiques qu'il entend mettre à la disposition des agents des services de renseignement et ce, tant pour faciliter leurs missions (avec, par exemple, un accès élargi aux fichiers) que pour les protéger juridiquement (par le renforcement de la préservation de leur anonymat dans le cadre des procédures judiciaires, par exemple).

Votre rapporteur pour avis est convaincu que le législateur, avec ce projet de loi de programmation militaire, dispose d'une opportunité historique de consolider la légitimité de nos services de renseignement, notamment en renforçant le contrôle parlementaire, ainsi que les moyens juridiques dont ils disposent.

Les amendements adoptés par la commission des Lois lors de sa réunion du 6 novembre dernier ont pour finalité de consolider et d'adapter le contrôle parlementaire et de renforcer le rôle du Premier ministre comme interlocuteur naturel de la délégation parlementaire au renseignement.

*

* *

Les **articles 4^{ter} à 4^{sexies}** contiennent des dispositions relatives au contrôle parlementaire de l'exécution de la loi de programmation. Ils ont été introduits dans le texte sur l'initiative de la commission des Affaires étrangères, de la défense et des forces armées du Sénat. L'**article 4^{quater}** prévoit que, chaque semestre, le ministre de la Défense présente aux commissions permanentes des deux assemblées un bilan de l'exécution de la loi de programmation. L'**article 4^{sexies}** prévoit un débat annuel au Parlement sur l'exécution de la présente loi de programmation militaire.

On peut s'interroger sur l'**article 4^{ter}**, qui propose de confier aux membres des commissions chargées de la défense de chaque assemblée des pouvoirs de contrôle sur pièces et sur place, qui sont actuellement exercés principalement par les rapporteurs spéciaux des commissions des Finances.

Cet article propose donc d'étendre au cas de l'application des lois de programmation militaire ces dispositions.

Ce faisant, le présent article crée une ambiguïté sur la nature du contrôle que les commissions chargées de la défense exerceraient. En matière budgétaire, c'est sur un fondement organique que repose la compétence des commissions chargées des finances. Mais, en dehors du contrôle de l'emploi des deniers publics, le législateur peut tout-à-fait prévoir des pouvoirs spécifiques.

De même, à l'**article 4 quinquies**, le Sénat propose que les communications faites par la Cour des comptes aux ministres soient non seulement transmises à la commission des Finances mais également, dans son champ de compétences, à la commission de la Défense, là aussi sans que cette possibilité soit prévue par un texte organique. Comme il n'existe aucune raison objective de réserver un sort particulier à cette commission, votre Commission propose d'étendre ce dispositif pour que les communications de la Cour des comptes soient transmises à chaque commission permanente des deux assemblées parlementaires, dans le respect de leur champ de compétences.

Les articles 5 à 13 comportent des dispositions relatives au renseignement.

L'**article 5** vise, précisément, à renforcer les prérogatives de la délégation parlementaire au renseignement. La délégation parlementaire au renseignement se verrait reconnaître la mission générale du « *contrôle parlementaire de l'action du Gouvernement en matière de renseignement* » et de l'évaluation de la politique publique en ce domaine.

Votre Commission a adopté plusieurs amendements ayant pour objectif de rendre plus cohérente et plus lisible la présentation des missions de la délégation parlementaire au renseignement. De la sorte, seront levées les ambiguïtés sur la nature des informations dont elle dispose.

Il est ainsi proposé que la délégation se voie communiquer « *des éléments d'information* » issus du plan national d'orientation du renseignement (sa déclinaison pour chaque service de renseignement leur permet d'orienter leur action), plutôt que le plan lui-même afin d'éviter qu'un autre document ne soit finalement élaboré dans le seul but d'éviter que certaines informations soient communiquées aux parlementaires.

Par ailleurs, votre Commission a souhaité que la délégation puisse solliciter du Premier ministre la communication de tout ou partie des rapports de l'inspection des services de renseignement, ainsi que des rapports des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence. Cette rédaction lui a paru plus opportune que celle retenue par le Sénat qui prévoit une transmission systématique des rapports d'inspection. En effet, une telle transmission pourrait être interprétée comme constituant une injonction au Gouvernement ⁽¹⁾, ce que la Constitution ne permet

(1) Dans sa décision n° 2009-581 DC du 25 juin 2009 sur une résolution tendant à modifier le Règlement de l'Assemblée nationale, le Conseil constitutionnel a considéré que le Règlement ne pouvait pas, sans méconnaître le principe de séparation des pouvoirs, permettre au comité d'évaluation et de contrôle des politiques publiques de l'Assemblée nationale de bénéficier du concours d'experts placés sous la responsabilité du Gouvernement (considérant n° 61) ; il s'agissait en l'occurrence des corps d'inspection comme, par exemple, l'inspection générale des finances ou des affaires sociales. Si le cas présent est clairement distinct, une disposition tendant à prévoir une transmission systématique de rapports d'inspections ministérielles pourrait être sujette à caution au regard du principe de séparation des pouvoirs.

pas. En outre, il n'a pas non plus paru opportun à votre Commission que la délégation se voie communiquer des rapports portant sur le détail de l'organisation des services, qui relève de la compétence des chefs de services, même si le contenu de certains de ces rapports peut lui être précieux. C'est pourquoi elle a permis que tout ou partie de certains rapports puisse lui être transmis par le Premier ministre, consacré ainsi comme l'interlocuteur naturel de la délégation parlementaire.

S'agissant de la composition de la délégation parlementaire au renseignement, il est proposé que les présidents des commissions chargées de la sécurité intérieure – les commissions des Lois – et de la défense ne soient plus membres de droit. Ils pourront naturellement être désignés par le président de l'assemblée concernée, si ce dernier le souhaite. L'objectif poursuivi est d'ouvrir la délégation aux parlementaires particulièrement intéressés par cette thématique. Les nominations s'effectueraient, comme aujourd'hui, de manière pluraliste.

Au cours du débat en commission, notre collègue Jean-Luc Warsmann, ancien président de la commission des Lois et, à ce titre ancien président de la délégation parlementaire au renseignement a approuvé la suppression des membres de droit. Il a cependant observé qu'il convenait que l'un des membres désigné appartienne à la commission des Lois, compétente en matière de sécurité intérieure.

Le Sénat a prévu que la délégation puisse entendre les agents des services de renseignement. Ce point a suscité un long débat au Sénat. Entendu par notre Commission le 30 octobre 2013 ⁽¹⁾, M. Patrick Calvar, directeur central du renseignement intérieur, a exprimé des réserves sur un tel dispositif. Il a ainsi estimé que si l'on permettait à la délégation parlementaire au renseignement d'entendre tout agent de ces services, « *il faudrait envisager une limite : le directeur de service doit pouvoir venir accompagné de la personne considérée comme la plus qualifiée* ». Il a ajouté qu'en outre, que si, « *du jour au lendemain, tout fonctionnaire sait qu'il est susceptible d'être entendu par la délégation parlementaire au renseignement, cela risque d'avoir des effets pervers sur le fonctionnement des services et sur la qualité de l'engagement des agents* ». Enfin, les services fonctionnant selon le principe du « besoin d'en connaître », le directeur central du renseignement intérieur a estimé que les « *réponses que les agents pourraient apporter à la délégation parlementaire au renseignement pourraient donc être tronquées, faute pour eux d'avoir une vision globale d'une situation* ».

Votre Commission propose, à l'instar d'ailleurs d'un sous-amendement du Gouvernement rejeté par le Sénat, que les directeurs puissent se faire accompagner, pour ces auditions, des collaborateurs de leur choix, mais en précisant que ce choix est guidé par « *l'ordre du jour de la délégation* ». Cette rédaction permettra à la délégation de disposer d'une information la plus complète

(1) Le compte rendu de cette audition figure dans le présent rapport.

possible, le responsable du service demeurant son interlocuteur naturel. Avec la rédaction proposée, la responsabilité du chef de service est consacrée ainsi que le pouvoir d'évocation de la délégation, par le biais de la communication de son ordre du jour.

La commission des Lois propose, enfin, que les observations et recommandations de la délégation adressées au président de la République et au Premier ministre soient également adressées au président de chaque assemblée, alors que le texte en vigueur ne prévoit qu'une simple transmission à leur égard. Il lui est apparu, en effet, paradoxal que la vocation d'un organe parlementaire soit d'informer, par priorité, l'exécutif.

L'article 6 prévoit de transformer la commission de vérification des fonds spéciaux en une formation spécialisée de la délégation parlementaire au renseignement.

Selon l'article 154 de la loi de finances pour 2002 n° 2001-1275 du 28 décembre 2001, la commission est « *chargée de s'assurer* » que les fonds spéciaux « *sont utilisés conformément à la destination qui leur a été assignée par la loi de finances* ». Elle a donc pour mission d'effectuer un contrôle de régularité des comptes des dépenses réalisées sur fonds spéciaux en s'assurant de la sincérité de leur imputation comptable. Il lui appartient ainsi de vérifier que ces fonds ont bien été utilisés pour financer des dépenses qui, en raison de leur nature particulière, ne sauraient être financées par un autre truchement.

Pour exercer ce contrôle, la commission de vérification des fonds spéciaux dispose de pouvoirs étendus : 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 présenter « *les registres, états, journaux, décisions et toutes pièces justificatives propres à l'éclairer* ».

La commission a la charge d'établir, pour chaque exercice budgétaire clos, un rapport sur les conditions d'emploi de ces fonds et un procès-verbal constatant que les dépenses réalisées sur ceux-ci sont couvertes par des pièces justificatives pour un montant égal. L'ensemble de ces documents est classifié.

Elle est composée de deux députés et deux sénateurs, désignés par le président de leurs assemblées respectives et de deux membres de la Cour des comptes. Cependant, depuis une décision de M. Philippe Séguin, alors premier président de la Cour, sur laquelle M. Didier Migaud n'est pas revenu, plus aucun magistrat de cette juridiction financière n'est nommé pour siéger à la commission de vérification des fonds spéciaux. Alors qu'il s'agit, en droit, d'une commission administrative, elle présente donc, dans les faits, l'apparence d'un organe parlementaire.

Tirant les conséquences du refus de la Cour des comptes de désigner des

représentants au sein de cette instance, la commission ne comprendrait plus, selon l'article 6 du projet de loi, de membres de la Cour des comptes, mais uniquement des parlementaires. Ses quatre membres seraient donc, par ailleurs, membres de la délégation parlementaire au renseignement.

Votre Commission a souhaité préciser que le choix des membres de la commission de vérification s'effectuerait de manière pluraliste. Cette formule lui a paru plus adaptée que celle retenue par le Sénat, qui reposait sur une parité entre majorité et opposition. En effet, si la notion d'opposition est connue ⁽¹⁾, tel n'est pas le cas de la notion de « *majorité* ».

Par ailleurs, pour souligner que la commission de vérification conservera ses spécificités et son identité, la commission des Lois propose de préciser que le poste de président de cette commission est maintenu et que son titulaire sera choisi chaque année.

Enfin, votre Commission a estimé nécessaire de préciser que le rapport de la commission de vérification est remis au Premier ministre et non pas à chacun des ministres concernés. Dans la même logique, il conforte la place du Premier ministre comme interlocuteur naturel des instances parlementaires en charge du renseignement. Elle a également prévu, comme c'est le cas aujourd'hui, l'information des présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances, mais en ne citant le président de la République et le Premier ministre – également destinataires de ce rapport – qu'après ces quatre membres des commissions chargées des finances, afin de montrer que la vocation d'un organe parlementaire n'est pas d'informer, par priorité, l'exécutif.

L'**article 7** permet l'audition d'agents des services de renseignement en dehors des tribunaux et des locaux des services enquêteurs afin de préserver leur anonymat.

Les **articles 8 et 9** étendent les possibilités, pour les agents de renseignement de consulter des fichiers administratifs.

L'**article 10** propose un fichier des passagers « *PNR* » ⁽²⁾ (ou *Passenger*

(1) Cette notion figure notamment dans les articles 48 et 51-1 de la Constitution. L'article 19 du Règlement de l'Assemblée nationale prévoit, dans ses alinéas 2 et 3, la possibilité pour les groupes parlementaires de déclarer leur appartenance à l'opposition. Une telle déclaration leur ouvre plusieurs « droits spécifiques » comme l'autorise depuis la révision constitutionnelle du 23 juillet 2008 l'article 51-1 de la Constitution. En application de l'article 19, alinéa 4 du Règlement, sont par ailleurs « considérés comme groupes minoritaires ceux qui ne se sont pas déclarés d'opposition, à l'exception de celui d'entre eux qui compte l'effectif le plus élevé ». Les groupes minoritaires se voient également reconnaître des droits spécifiques en vertu du même article de la Constitution.

(2) Ces données peuvent comprendre : les nom et prénom du passager, les renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, l'itinéraire du déplacement qui peut comporter plusieurs étapes, les indications des vols concernés, le nombre de personnes pour lesquelles une même réservation est faite, les coordonnées de contact du passager, les tarifs accordés, l'état du paiement effectué et ses modalités, les réservations d'hôtels ou de voitures à l'arrivée ou encore les services demandés à bord.

name record) français, dans l'attente de la publication d'une directive européenne. Ce fichier serait placé sous la responsabilité des ministres chargés de l'intérieur, de la défense, des transports et des douanes. Il serait mis en œuvre, comme le prévoirait la directive, par une « unité d'information passagers » composée de membres des services de la douane, de la police et de la gendarmerie.

La commission des Lois propose de garantir, par un amendement, que les données « sensibles » soient exclues des données transmises. Il s'agit des données à caractère personnel susceptibles de révéler l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, ou les données qui concernent la santé ou la vie sexuelle de l'intéressé.

Les **articles 11 et 12** permettent l'accès des services du ministère de la Défense aux fichiers de police judiciaire dans le cadre des enquêtes administratives ou d'interventions.

L'**article 13**, qui est un article extrêmement important, tend à clarifier le cadre juridique relatif à la géolocalisation en temps réel des téléphones ou d'autres terminaux électroniques tels que des ordinateurs.

La commission des Lois du Sénat a, en effet, estimé que la géolocalisation en temps réel d'une personne semblait plus proche, en termes d'atteinte aux libertés, de l'interception d'une communication que du simple recueil de données de connexion⁽¹⁾. Elle a également observé que le fait que la géolocalisation soit insérée dans l'article L. 34-1-1 du code des postes la cantonnait à un usage anti-terroriste – cet article portant exclusivement sur cet objet –, alors même que les services de renseignement pourraient en avoir besoin pour les finalités beaucoup plus larges prévues par le dispositif issu de la loi du 10 juillet 1991⁽²⁾. Elle a donc opéré la fusion des dispositifs de recueil des données de connexions, sur le modèle applicable aux interceptions de sécurité.

Votre Commission propose d'aller jusqu'au bout de cette logique d'analogie avec les interceptions de sécurité. En effet, le texte du Sénat a souhaité que la géolocalisation soit une mesure d'une durée de 10 jours renouvelable. Elle a donc adopté un amendement qui aligne cette durée sur celle des interceptions de sécurité, soit quatre mois afin de permettre aux services de tirer tout le profit nécessaire de cette géolocalisation qui suppose souvent, pour être efficace, un suivi sur plusieurs semaines des personnes surveillées.

Les **articles 14, 15, 16, 16 bis et 16 ter** comportent des dispositions

(1) Ces données sont celles figurant sur les factures détaillées (identité des personnes entrées en communication, date et durée de l'échange), celles permettant de localiser un téléphone portable ou un ordinateur, mais aussi les données de connexion Internet (numéro de protocole, date et durée des connexions).

(2) Il s'agit de la sécurité nationale, de la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous.

relatives à la protection des infrastructures vitales contre la cybermenace.

Les articles **17 à 21** comportent des dispositions relatives au traitement pénal des affaires militaires. Votre rapporteur pour avis souligne que l'**article 17** instaure une présomption simple, selon laquelle la mort violente d'un militaire, au cours d'une action de combat lors d'une opération militaire, est présumée ne pas avoir une cause inconnue ou suspecte. S'agissant d'une présomption simple, l'officier de police judiciaire des forces armées ne pourra ouvrir d'enquête sur les recherches de cause de la mort que s'il apporte des éléments selon lesquels les circonstances de la mort sont inconnues ou suspectes.

L'**article 18** propose de confier au ministère public le monopole de la mise en mouvement de l'action publique, pour tout fait commis par un militaire dans le cadre de sa mission, lors d'une « *opération militaire se déroulant hors du territoire français* ». L'**article 19** améliore le régime particulier de mise en cause de la responsabilité pénale des militaires. L'**article 20** procède à la correction d'erreurs formelles résultant de la suppression du Tribunal aux armées de Paris et apporte des précisions sur la procédure pénale applicable aux militaires en temps de paix. L'**article 21** vise à rationaliser la carte judiciaire des juridictions de droit commun spécialisées en matière militaire.

Enfin, l'**article 22** propose une extension de la protection fonctionnelle ⁽¹⁾ aux ayants-droit des militaires décédés en opérations et à certains personnels civils.

*

* *

(1) La protection fonctionnelle est la protection, par la puissance publique, de ses agents dans l'exercice de leurs fonctions, en cas de mise en cause par des tiers. Ce soutien exprime un rapport de solidarité entre l'agent et son administration et ce, dans l'intérêt du service. Il peut prendre la forme de la prise en charge des frais d'avocat, par exemple.

AUDITION DE M. ALAIN ZABULON, COORDONNATEUR NATIONAL DU RENSEIGNEMENT

Lors de sa réunion du mercredi 9 octobre 2013, la Commission procède à l'audition de M. le préfet Alain Zabulon, coordonnateur national du renseignement.

M. le président Jean-Jacques Urvoas. Mes chers collègues, nous accueillons aujourd'hui M. le préfet Alain Zabulon, qui est coordonnateur national du renseignement.

Son audition n'est pas ouverte à la presse ni retransmise sur le canal interne de l'Assemblée nationale. Elle ne sera pas non plus diffusée sur le site internet de celle-ci. Les propos qui y seront tenus, en particulier par M. le coordonnateur, ne pourront donc pas faire l'objet de *tweets*. C'est une question de confiance réciproque à l'égard de notre interlocuteur quant aux informations qu'il pourrait délivrer aux membres de la Commission. Un compte-rendu écrit sera néanmoins publié à l'issue de cette audition.

Monsieur le coordonnateur national, M. Jean-Luc Warsmann, qui présidait la commission des Lois sous la précédente législature, avait souhaité recevoir vos prédécesseurs. Cela n'a pu se faire, en raison de l'emploi du temps très chargé de la Commission.

Nous bénéficions ici d'une opportunité législative : l'examen, en cours au Sénat, et bientôt devant notre assemblée, du projet de loi de programmation militaire (LPM), dont plusieurs articles concernent le renseignement. C'est la raison pour laquelle la commission des Lois s'est saisie pour avis de ce projet de loi et a désigné comme rapporteur pour avis M. Patrice Verchère, qui a déjà été co-rapporteur d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, mission créée par notre Commission et qui a rendu ses conclusions en mai dernier.

Je vous demande de bien vouloir nous présenter, en les dessinant à grands traits, les différents services composant la communauté du renseignement et que vous avez pour mission de coordonner auprès du président de la République ainsi que la fonction qui est la vôtre et qui a été créée sous le mandat de Nicolas Sarkozy. Je tiens à rappeler à cet égard que le renseignement a une définition juridique précise. Quelles sont par ailleurs les propositions du Gouvernement en la matière figurant dans le projet de loi de programmation militaire ? De quels pouvoirs et compétences supplémentaires le contrôle parlementaire sera-t-il pourvu ? Monsieur le coordonnateur national, je vous cède la parole.

M. Alain Zabulon, coordonnateur national du renseignement. Je tiens tout d'abord à remercier le président Jean-Jacques Urvoas de me donner

l'occasion, c'est la première fois, de m'exprimer devant la commission des Lois de l'Assemblée nationale et de mieux faire connaître ce qu'est l'activité des services de renseignement. La communauté nationale du renseignement étant une institution mal connue en dehors de quelques spécialistes, je tiens à vous en brosser les contours avant d'évoquer les principales dispositions du volet renseignement du projet de loi de programmation militaire.

Les services de renseignement sont au nombre de six.

Il existe tout d'abord deux grands services à vocation généraliste, la Direction générale de la sécurité extérieure (DGSE) et la Direction centrale du renseignement intérieur (DCRI).

La DGSE a pour mission de rechercher et d'exploiter les renseignements qui intéressent la sécurité de notre pays et de détecter et d'entraver hors du territoire national des activités d'espionnage dirigées contre les intérêts français afin d'en prévenir les conséquences. Comme son nom l'indique, la DGSE est un service qui assure la sécurité des intérêts de la France à l'extérieur grâce aux informations qu'elle recueille.

La DCRI, elle, a compétence pour lutter sur le territoire de la République contre toutes les activités qui sont susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation. À ce titre, elle a pour mission de détecter les risques de menaces terroristes, notamment d'attentats, en surveillant des individus dont il est avéré ou dont on peut penser qu'ils sont susceptibles de commettre des actes hostiles à la sécurité et aux intérêts fondamentaux de la nation. Cette mission de renseignement intérieur englobe tous les aspects relatifs à la sécurité du territoire.

La DCRI est le fruit de la fusion de l'ancienne Direction de la sécurité du territoire (DST) avec une partie de la Direction centrale des renseignements généraux (DCRG), direction qui a disparu – les renseignements généraux n'existent plus –, l'autre partie des RG ayant rejoint la Sous-direction de l'information générale (SDIG), qui pratique, dans les territoires, la collecte des informations nécessaires aux préfets.

Il existe quatre autres services, plus spécialisés.

La Direction du renseignement militaire (DRM), qui est à la disposition du chef d'état-major des armées, recueille toutes les informations nécessaires sur les théâtres d'opérations pour permettre aux forces armées de se déployer et d'agir dans les meilleures conditions. Elle dispose à cet effet de moyens d'observation très développés – des satellites, des avions, des drones de nouvelle génération qui remplaceront le parc actuel qui est en voie d'obsolescence – qui permettent de guider les forces armées au sol dans leur déploiement.

La Direction de la protection de la sécurité de la défense (DPSD), sous la tutelle du ministre de la Défense, assure la sécurité du personnel militaire, des

informations détenues et maniées par le ministère de la Défense, du matériel et des installations sensibles. Elle garantit en quelque sorte la sécurité de l'« outil défense ».

La Direction nationale du renseignement et des enquêtes douanières (DNRED) a pour priorité de lutter notamment contre la grande fraude douanière, la criminalité organisée et les trafics en tous genres – drogues, marchandises diverses ou armes –, dont la circulation est favorisée par la mondialisation.

Tracfin – Traitement du renseignement et action contre les circuits financiers clandestins –, enfin, est une cellule de renseignement financier qui recueille et analyse tous les renseignements propres à établir l'origine et la destination de sommes ayant fait l'objet d'une déclaration de soupçon. Tracfin est un service qui est alimenté par les déclarations auxquelles certaines professions sont tenues de procéder, notamment dans le secteur bancaire. Ce service enquête sur les transactions financières, dont l'origine ou la destination sont sujettes à soupçon et peut saisir le procureur de la République s'il soupçonne une infraction.

Ces six services forment la « communauté nationale du renseignement », qui est une formule originale. En effet, trois de ces services, la DGSE, la DRM et la DPSD, sont placés sous l'autorité du ministre de la Défense, tandis que la DCRI est placée sous celle du ministre de l'Intérieur et la DNRED et Tracfin sous celle du ministre de l'Économie. Ils sont donc clairement placés sous l'autorité de leur ministre de tutelle : il n'existe pas, dans le système français, de « superchef » des services de renseignement. Il s'agit d'une organisation administrative classique de grandes directions qui sont des services publics placés sous l'autorité des ministres. Toutefois, comme les services composant la communauté du renseignement ont des sujets communs à traiter, le décret du 24 décembre 2009 a créé la fonction de coordonnateur national du renseignement, qui est placé auprès du président de la République.

La première mission du coordonnateur est de veiller à la qualité de l'information transmise par les services de renseignement au chef de l'État. Tous les jours, les six services que j'ai décrits font remonter des notes et des informations sur les sujets d'actualité. S'agissant de l'extérieur, les notes les plus abondantes portent à l'heure actuelle sur la Syrie, le Mali, la République Centrafricaine ou les événements dramatiques qui se sont déroulés au Kenya. En matière de sécurité intérieure, les notes portent essentiellement sur les risques liés aux groupes islamistes radicaux susceptibles de provoquer des attentats et de se livrer à des activités de terrorisme. Le rôle du coordonnateur est de veiller tous les jours à coordonner et à mettre en forme ces multiples informations et à les adresser au président de la République qui, tous les soirs, trouve sur son bureau une note qui fait la synthèse des informations adressées par les services de renseignement.

La deuxième mission du coordonnateur est de définir et de hiérarchiser les priorités : l'action des services de renseignement s'inscrit dans un cadre fixé par le

Gouvernement et tracé dans un document classifié « secret défense » et intitulé « Plan national d'orientation du renseignement » (PNOR). Ce document, qui définit les priorités d'action des services, constitue leur feuille de route. Le PNOR est rédigé par le coordonnateur national du renseignement et son équipe en étroite concertation avec les services.

Je tiens à vous faire part de la création, cette année, d'un nouveau document d'orientation générale, intitulé « Stratégie nationale du renseignement », qui, lui, sera rendu public. Il permettra de communiquer sur les grandes priorités des services de renseignement pour les deux ou trois ans à venir. Il est en cours d'élaboration en concertation avec les cabinets des ministres concernés.

La troisième mission du coordonnateur est d'être l'interlocuteur privilégié du Premier ministre et des cabinets ministériels concernés en matière de renseignement. Ainsi, dans le cadre de l'adoption de la prochaine loi de programmation militaire, le coordonnateur national du renseignement est associé à toutes les réunions interministérielles où sont examinées les propositions d'amendements. Il fait en permanence le lien avec les services de renseignement pour les informer du cheminement du texte et recueillir leur avis sur une disposition ou sur une proposition d'amendement.

Le coordonnateur est également l'interlocuteur de la délégation parlementaire au renseignement (DPR), qui a été créée en 2007 et est composée de huit parlementaires, quatre députés et quatre sénateurs. La prochaine loi de programmation militaire donnera à cette délégation des prérogatives renforcées puisqu'elle sera chargée du contrôle de l'activité du Gouvernement dans le domaine du renseignement. C'est un grand progrès que le Parlement, par l'entremise de sa délégation spécialisée, s'intéresse au monde du renseignement, qui a souvent souffert, à tort, d'une réputation sulfureuse en raison d'affaires ayant défrayé la chronique. Or les services de renseignement participent de la politique de sécurité globale et il est bon que le Parlement s'y intéresse. Je tiens à souligner la qualité de la collaboration et des rapports de confiance qui se sont instaurés entre la communauté du renseignement et la délégation parlementaire depuis sa création.

Le coordonnateur – c'est sa quatrième mission – veille également à la bonne utilisation des moyens alloués aux services de renseignement. Des arbitrages budgétaires assez favorables ont été rendus dans le cadre de la loi de programmation militaire et la communauté du renseignement s'est engagée dans une politique dynamique de mutualisation des moyens qui lui sont alloués. Le monde du renseignement n'échappe pas à la « course aux armements » : l'évolution des moyens techniques d'investigation et d'interception rend nécessaires des investissements très coûteux. C'est pourquoi chaque euro affecté à la communauté du renseignement est, dès que les conditions sont remplies, mutualisé entre plusieurs services de manière à ce que ceux-ci ne soient pas tentés, notamment, de disposer de leurs propres dispositifs informatiques ou d'interception.

Je tiens aussi à rappeler que les services de renseignement sont contrôlés puisqu'ils sont des administrations de l'État. Il existe cinq niveaux de contrôle.

Les agents des services de renseignement, y compris à l'autre bout du monde, agissent tout d'abord sous le contrôle de leur hiérarchie, qui rend compte au ministre de tutelle. Les corps d'inspection exercent eux aussi leur propre contrôle de ces services. Du reste, un décret créant une inspection spécialisée pour les services de renseignement devrait être publié avant la fin de l'année 2013. Cette inspection regroupera les compétences de l'inspection générale de l'administration du ministère de l'Intérieur, de l'inspection générale des finances et du contrôle général des armées du ministère de la Défense. Elle conduira, outre des missions de contrôle, des missions d'audit, d'évaluation et de conseil des services de renseignement.

La France étant un État de droit, le monde du renseignement n'est pas non plus à l'abri du juge, qu'il s'agisse du juge des comptes ou du juge pénal. Les services de renseignement ne bénéficient donc d'aucun régime d'irresponsabilité pénale, même si certaines dispositions protègent les agents, par exemple ceux qui infiltrent des groupes particulièrement dangereux et qui bénéficient d'une fausse identité ou de mesures spécifiques de protection.

Le Parlement, par l'entremise de la délégation parlementaire au renseignement, contrôle, quant à lui, non pas directement les services de renseignement mais l'activité du Gouvernement dans le domaine du renseignement.

Enfin, des autorités administratives indépendantes participent à la régulation de l'activité de la communauté du renseignement. La Commission nationale de contrôle des interceptions de sécurité (CNCIS), créée par la loi du 10 juillet 1991, émet un avis sur toutes les demandes d'écoutes formulées par les services de renseignement. La Commission nationale informatique et libertés (CNIL) suit les fichiers détenus par les services de renseignement et fait des contrôles sur pièces et sur place à l'occasion du droit d'accès indirect ouvert aux tiers.

Tels sont les cinq niveaux de contrôle des services de renseignement.

La communauté du renseignement est entrée dans une phase très active de collaboration entre les services, qui ne connaissent pas la « guerre des polices ». Les relations, les coopérations et les échanges d'informations n'ont jamais été aussi intenses et poussés qu'aujourd'hui. Je peux en témoigner à propos de la crise syrienne, la première dont j'ai assuré le suivi en tant que coordonnateur national du renseignement : les informations précises et fiables qui sont remontées au président de la République ont joué un rôle très important dans le processus de prise de décision et dans la définition de la position de la France.

Voici, rapidement exposé, le panorama du renseignement en France. Je me tiens à votre disposition pour répondre à vos questions.

M. Patrice Verchère, rapporteur pour avis. Monsieur le coordonnateur, à la suite des préconisations que le président de notre Commission, M. Jean-Jacques Urvoas, et moi-même avons formulées dans un rapport d'information publié en mai dernier, rapport qui a été adopté à l'unanimité de la Commission, je souhaite vous poser trois questions sur le projet de loi de programmation militaire, dont je serai le rapporteur pour avis.

S'agissant des fichiers, je me félicite de la création d'un traitement relatif aux données des transporteurs aériens – notre collègue Guy Geoffroy a d'ailleurs beaucoup travaillé sur la question. Je ne doute pas que ce dispositif, prévu jusqu'au 31 décembre 2017, sera prorogé compte tenu de son utilité.

En ce qui concerne plus particulièrement l'accès des agents de renseignement à certains fichiers de police, prévu par les articles 11 et 12 du projet de loi de programmation militaire, pouvez-vous nous indiquer les bénéfices attendus en la matière par les services de renseignement ?

Le rapport d'information avait pointé les lacunes en matière de géolocalisation des téléphones mobiles des personnes suspectées de terrorisme. Le dispositif proposé à l'article 13 du projet de loi de programmation militaire répond-il aux attentes des services de renseignement ?

Sur l'anonymat des agents, enfin, l'article 27 de la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) du 14 mars 2011, adopté sur l'initiative de la précédente majorité avec l'appui de l'opposition, a institué un régime de déposition spécifique aux personnels des services de renseignement qui peuvent être témoins, dans le cadre de leurs missions, de la commission d'une infraction. On sait toutefois que des terroristes ont réussi à établir des listes d'agents, notamment en recoupant des noms figurant dans des procès-verbaux judiciaires.

Il est donc proposé de modifier de nouveau le code de procédure pénale pour que l'audition d'un agent se déroule dans un lieu « assurant l'anonymat et la confidentialité ». Cette rédaction permettra-t-elle de garantir effectivement l'anonymat de nos agents ?

Mme Marietta Karamanli. Plusieurs personnalités françaises plaident depuis plusieurs années pour une mutualisation européenne de la politique du renseignement sous la houlette de la Commission européenne.

En juillet dernier, la presse a affirmé que l'Union européenne veut créer sa propre agence du renseignement et de défense, activité pour laquelle elle envisagerait un usage intensif de drones espions et de satellites. Cette agence serait dirigée par le Haut représentant de l'Union européenne pour les affaires étrangères et la politique de sécurité.

Or le traité de Lisbonne prévoit de manière explicite que le renseignement relève exclusivement du domaine régalien des États. L'article 3 *bis* du traité

précise que « la sécurité nationale reste de la seule responsabilité de chaque État membre ».

Quelle est la position défendue par la France en la matière ?

M. Alain Zabulon. L'article 8 du projet de loi de programmation militaire harmonise et aligne le droit d'accès de l'ensemble des services de renseignement aux fichiers administratifs, ce droit d'accès étant déjà reconnu aux services relevant du ministère de l'Intérieur. Il s'agit notamment du fichier national des immatriculations, du système national des permis de conduire ou du système de gestion des cartes d'identité.

Par ailleurs, l'article 11 du projet de loi permettra aux services qui ne le pouvaient pas encore, de recourir aux fichiers de police judiciaire, notamment dans le cadre des enquêtes d'habilitation au secret de la défense nationale. Au plan opérationnel, les agents de renseignement sont parfois au contact, pour des raisons liées à leurs missions, d'individus dangereux ou d'interlocuteurs peu recommandables. Aussi est-il préférable qu'ils sachent à qui ils ont affaire, notamment lorsqu'ils doivent passer à une phase d'interpellation ou d'infiltration dans un groupe. L'article 11 permettra à l'ensemble des services de renseignement de savoir si les individus dont ils s'occupent ont un passé judiciaire en France. Cette disposition améliorera l'efficacité des services.

J'insiste sur le fait que, si l'accès par les services de renseignement aux fichiers est facilité, dans un souci de respect des libertés individuelles, la Commission nationale de l'informatique et des libertés (CNIL) continuera de s'assurer que ces fichiers ne sont pas consultés à d'autres fins que celles prévues dans la loi. Chaque consultation des fichiers fera l'objet d'une traçabilité : seuls des agents habilités pourront consulter les fichiers et la CNIL pourra exercer des contrôles *a posteriori* tels que définis par la loi.

S'agissant de l'anonymat des agents, le projet de loi vise à améliorer les conditions dans lesquelles un agent peut être auditionné dans le cadre d'une procédure judiciaire. L'article 7 prévoit qu'en cas de risque pour son identité l'audition de l'agent pourra être effectuée dans un lieu assurant son anonymat et la confidentialité de l'échange avec l'autorité judiciaire. Ce lieu sera choisi par le chef du service de l'agent et pourra être celui du service d'affectation de ce dernier.

S'agissant de la géolocalisation, je tiens à rappeler que la loi de juillet 1991 visait à encadrer juridiquement les interceptions de sécurité, c'est-à-dire les écoutes téléphoniques qui peuvent être autorisées après avis de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) et sur décision du Premier ministre. La loi de 1991 n'avait évidemment pas anticipé l'arrivée d'internet et des réseaux sociaux. Au fil du temps, les données de connexion – l'adresse IP, le nom de l'appelant ou de l'appelé, les fadettes, etc. – ont constitué une mine d'informations de plus en plus précieuses auxquelles il faut

pouvoir accéder dans le cadre de la lutte contre le terrorisme, en vue, notamment, de renseigner l'itinéraire d'un individu faisant partie d'un groupe susceptible de commettre un attentat.

La loi de 1991 ayant atteint ses limites, le président de la CNCIS a souhaité que la loi encadre la géolocalisation qui, je le rappelle, est un procédé intrusif puisqu'elle permet en temps réel une filature électronique d'un individu *via* son téléphone mobile. Si la loi antiterroriste du 23 janvier 2006 a donné un fondement juridique à la géolocalisation, l'article 13 du projet de loi de programmation militaire va plus loin en mentionnant explicitement le recours à la géolocalisation en temps réel comme possibilité de prévention des risques d'attentat. Cet article ne fait toutefois qu'une partie du chemin puisqu'il n'élargit pas cette possibilité aux autres motifs inscrits dans la loi de 1991 et qu'il n'autorise « expressément » que « les services de police et de gendarmerie chargés de la prévention du terrorisme à accéder en temps réel à des données de connexion mises à jour ». Le Gouvernement est conscient de la nécessité de poursuivre la réflexion sur ce sujet afin d'aboutir à un dispositif juridique global et harmonisé.

Pour répondre à la question de Mme Karamanli, le Gouvernement considère que le renseignement doit rester une compétence des États. Il est opposé à ce qu'il remonte au niveau communautaire car il remplit des missions de souveraineté. Lorsque le Gouvernement doit définir sa position dans des crises internationales, il est essentiel que l'information lui soit apportée par ses services de renseignement. En 2003, pour refuser de participer à la guerre contre l'Irak, la France s'est appuyée sur les informations de ses propres services, pour lesquels il n'était pas avéré que le gouvernement irakien de l'époque possédait des armes de destruction massive. Plus récemment, les services de renseignement ont fait un travail très approfondi de collectes d'informations sur le conflit syrien, permettant au président de la République et au Gouvernement de se forger la conviction de l'implication du régime syrien dans le bombardement chimique du 21 août. Pour la première fois, le Gouvernement a accepté de déclassifier des notes – le document est présent sur le site internet du Premier ministre – permettant d'expliquer comment il était arrivé à la conviction que l'attaque chimique était le fait de l'État syrien. Si le Gouvernement n'est pas informé par ses propres services, sa position sera moins assurée. C'est une chose de collaborer avec des services de renseignement étrangers – nous travaillons beaucoup avec les services de renseignement britanniques, allemands ou américains – c'en est une autre d'entrer dans la voie de l'Europe du renseignement. Ce n'est pas celle, en tout cas, qu'a choisie le Gouvernement.

M. Guillaume Larrivé. L'émergence de la DGSI – Direction générale de la sécurité intérieure –, parallèle à la Direction générale de la police nationale (DGPN), pose la question de la réorganisation du réseau territorial des services de renseignement. Comment l'articulation des ex-SDIG et des ex-antennes de la DCRI se mettra-t-elle en œuvre au niveau zonal comme à ceux de la région et du département ?

M. Alain Zabulon. Je rappelle que la DCRI est née de la fusion de l'ex-DST avec une partie de la DCRG, l'autre partie des renseignements généraux ayant donné naissance à la SDIG, sous-direction de l'information générale, dont la mission est de renseigner les représentants de l'État dans les départements et les régions sur tous les événements touchant à l'actualité économique et sociale – les conflits sociaux, les mouvements de grève, les entreprises en difficulté. Les SDIG ne participent à aucune activité en matière de renseignement politique, notamment électoral. Au moment des élections, le Gouvernement demande aux préfets de se livrer à des pronostics : les SDIG n'interviennent plus en la matière – c'était le cas par le passé, cela ne l'est plus. Leur mission, je le répète, est centrée sur les événements économiques et sociaux et, dans les grandes agglomérations, sur les phénomènes de bande au sein des quartiers sensibles où, sous l'autorité des directeurs départementaux de la sécurité publique (DDSP), les SDIG suivent à la criminalité organisée.

La DCRI deviendra, comme vous l'avez mentionné, la Direction générale de la sécurité intérieure (DGSi) : ce n'est pas qu'un changement de nom puisque actuellement la DCRI est une des directions de la grande Direction générale de la police nationale (DGPN). En devenant à son tour une direction générale de plein exercice, la DGSi prendra son autonomie par rapport à la DGPN, dans le cadre d'une montée en puissance sur le plan qualitatif. En effet, à l'heure actuelle, la DCRI recrute essentiellement dans la sphère policière, alors que, pour être efficace dans le renseignement, la DCRI a besoin de regrouper d'autres spécialités : des analystes de haut niveau, des informaticiens, des interprètes ou des spécialistes en propriété industrielle. Or son statut de direction adossée à la DGPN ne lui permet pas de recruter aussi facilement que nécessaire ces compétences rares. La nouvelle DGSi pourra le faire plus aisément.

Quant au renseignement territorial, la SDIG deviendra le Service central du renseignement territorial (SCRT), qui continuera d'assurer l'information des préfets. Toutefois, comme la collaboration et l'échange d'informations au plan local entre les services départementaux d'information générale et le renseignement intérieur ne sont pas toujours optimaux, notamment dans le suivi des quartiers sensibles, il est prévu au niveau zonal – la France métropolitaine est coupée en sept zones – la création d'une instance de coordination entre le renseignement territorial et le renseignement intérieur permettant de faire redescendre l'information jusqu'aux préfets de départements.

Je vous donne un exemple concret. Lorsqu'un jeune, qui fait partie d'une bande de quartier et est donc suivi par la DDSP et la SDIG, bascule dans l'extrémisme radical et envisage de faire le voyage initiatique en Syrie – plus de 130 jeunes Français sont actuellement sur les théâtres d'opérations syriens –, son suivi passe alors à la DCRI. Des conflits de compétence étant donc actuellement possibles entre le renseignement territorial et le renseignement intérieur, il est du plus haut intérêt de créer cet échelon de coordination, au-delà de la première étape mise en place par le ministre de l'Intérieur début 2013 pour renforcer la coordination entre les échelons locaux, zonaux et centraux de la DCRI et des

SDIG, pour ne pas manquer de repérer un futur Mohamed Merah. Cet échelon assurera la continuité de l'information entre le renseignement territorial et le renseignement intérieur. Tel est l'objet de la réforme entreprise par le ministre de l'Intérieur qui attache la plus haute importance à ce projet.

M. le président Jean-Jacques Urvoas. J'ai une question à vous poser sur le périmètre de la communauté du renseignement. En effet, d'autres services que ceux que vous avez évoqués concourent au renseignement. Vous avez évoqué les services départementaux d'information générale qui formeront le SCRT. Certains personnels de la préfecture de police de Paris ont également sur le territoire francilien les mêmes compétences que les agents de la DCRI : ils font du renseignement, tout comme la gendarmerie, rattachée au ministère de l'Intérieur depuis la loi de 2009.

Envisagez-vous de conseiller au Gouvernement une évolution du périmètre de la communauté du renseignement ? Je tiens également à évoquer l'Académie du renseignement, une excellente structure qui a été créée au cours du précédent mandat présidentiel et dont la vocation est de doter tous les agents de renseignement d'une culture commune. La Délégation parlementaire au renseignement reçoit chaque année depuis sa création des agents de cette académie, ce qui a permis aux membres de la délégation de dire notre attachement aux services que ces agents rendent à la patrie.

Enfin, certains jeunes semblent plus attirés par la Syrie qu'ils ne l'ont été par l'Afghanistan ou le Mali. Combien de jeunes sont actuellement suivis dans le cadre de ce que vous appelez le « voyage initiatique » en Syrie ?

M. Alain Zabulon. Le périmètre de la communauté du renseignement n'est pas figé. Les six services que j'ai mentionnés ont pour point commun de recueillir de l'information par des moyens couverts par le secret défense, y compris clandestinement – c'est la marque de fabrique de ces services. Toutefois, une partie de la direction du renseignement de la préfecture de police de Paris réalise un travail voisin, en lien, du reste, avec la DCRI. On pourrait donc à bon droit réfléchir à un éventuel élargissement du périmètre à cette direction. Si le président de la République n'a pas procédé à un tel élargissement lors du conseil national du renseignement du 10 juin 2013, la question n'en reste pas moins ouverte.

La question l'est également pour le renseignement territorial, compte tenu des indispensables échanges d'informations avec le renseignement intérieur pour tout ce qui touche aux intérêts fondamentaux de la nation. Des passerelles peuvent être imaginées. Il n'y a pas à l'heure actuelle de projets de textes précis tendant à élargir la communauté du renseignement. En qualité de coordonnateur du renseignement, si le président de la République ou le Premier ministre me posaient la question, je répondrais qu'il convient de créer des formes de collaboration entre tous ces services, dans le seul objectif d'améliorer l'efficacité globale des politiques de prévention et de sécurité.

Vous avez eu raison, monsieur le président, d'évoquer l'Académie du renseignement. Cette institution joue un rôle très important dans la formation de l'esprit communautaire du renseignement. Elle dispense des formations de grande qualité. Si des parlementaires sont intéressés à participer à une séquence de sensibilisation ou de formation sur le renseignement, je leur ouvre volontiers les portes de l'Académie dans le cadre d'un module organisé à leur attention. Je me félicite, je le répète, du fait que la représentation nationale s'intéresse au monde du renseignement.

La « filière syrienne » est aujourd'hui notre principale source de préoccupation. Chaque fois que la France a été engagée sur un théâtre d'opérations, que ce soit militairement – comme en Afghanistan ou au Mali – ou diplomatiquement – c'est le cas de la Syrie –, nous avons assisté à la création de filières de jeunes gens qui, issus de la deuxième ou troisième génération de l'immigration ou convertis à l'islam, espèrent en application d'une lecture radicale de leur religion donner un sens à leur vie dans le cadre d'un voyage initiatique. Ils consultent des sites djihadistes sur internet, se laissent influencer puis franchissent l'étape du départ. Il y en a eu une vingtaine en Afghanistan et très peu au Mali en raison de l'opération Serval : ils sont en revanche quelque 138 en Syrie et ce chiffre est en constante augmentation. C'est un vrai sujet de préoccupation parce que ces jeunes ne rejoignent pas la Coalition nationale syrienne ou l'Armée syrienne libre soutenues par ses alliés mais les groupes djihadistes, notamment *Jabhat al-Nosra* ou l'État islamique de l'Irak et du Levant, au contact desquels ils acquièrent un état d'esprit qui constitue une menace lors de leur retour en France. Un peu plus de 300 individus font l'objet d'un suivi et, je le répète, 138 sont présents sur les théâtres d'opération, une dizaine d'entre eux y ayant d'ailleurs perdu la vie. Certains sont également en transit. Il faut savoir qu'il est très facile d'aller en Syrie, la frontière turque étant très poreuse – aujourd'hui, quelque 3 000 étrangers sont présents en Syrie, dont 600 Européens.

Les djihadistes, qui ont parfaitement compris le parti qu'ils pouvaient tirer de cette « main-d'œuvre » composée de jeunes gens volontaires, leur donnent souvent la consigne de retourner dans leur pays d'origine pour y pratiquer le djihad. C'est un vrai sujet de sécurité intérieure auquel il faut être très attentif, tout en ayant soin, bien entendu, d'éviter, dans nos prises de parole publiques, et pour ma part, j'y veille constamment, tout amalgame avec la communauté musulmane qui souffre dans son ensemble de ces comportements marginaux et désapprouve ces errements individuels qui constituent une menace importante.

M. Christian Assaf. Quelle est la nature de la coopération entre les services de renseignement français et ceux des pays amis ?

M. Alain Zabulon. Les coopérations bilatérales avec les services étrangers sont nombreuses et constantes, notamment avec les services américains sur la Syrie et le Mali, avec les services britanniques et les services allemands.

Par ailleurs, mes homologues étrangers de passage à Paris viennent

toujours me rencontrer : je reçois régulièrement des responsables d'autres services de renseignement étrangers – je pense au *Director of National Intelligence* américain ou au directeur de la *CIA* que j'ai rencontré récemment. Ces contacts m'ont permis de mesurer combien les services de renseignement français sont considérés parmi les meilleurs au monde, notamment par les pays qui sont nos alliés dans la gestion des crises actuelles. Cette collaboration, qui se fait de service à service, crée un réseau qui nous permet d'instaurer sans difficulté aucune, en cas de crise, des échanges d'informations. De plus, en pratiquant la collaboration bilatérale, nous ne nous défaisons en rien d'une compétence de souveraineté au profit de l'Union européenne.

M. le président Jean-Jacques Urvoas. Cette législature doit permettre de franchir un nouveau pas dans la relation entre le Parlement et les services de renseignement, après leur découverte mutuelle sous la précédente législature. Désormais, la confiance existe entre la communauté du renseignement et les parlementaires siégeant dans la délégation parlementaire au renseignement. Nous changerons sans doute le texte de la loi puisque aujourd'hui la délégation n'est chargée que du suivi des services et que, demain, elle le sera du contrôle des services. L'opinion comme les services gagneront au franchissement de cette étape supplémentaire : l'opinion, qui aura ainsi la garantie que la communauté du renseignement n'est pas dévoyée vers d'autres missions que celles que lui assignent la loi, et les services qui seront protégés à la fois sur le plan pénal et face à la presse. J'ai, à cet égard, regretté personnellement – la délégation parlementaire au renseignement l'a dit au Premier ministre – que le Gouvernement n'engage pas d'action contre les journaux qui publient les noms des personnels du renseignement – *Paris-Match* a ainsi publié le nom du capitaine qui dirigeait le commando parti en Somalie libérer notre otage : il n'est pas acceptable que le Gouvernement n'ait pas entamé une action contre cette publication car il convient de protéger les personnels des services de renseignement. Victor Hugo disait qu'« *il n'est rien au monde d'aussi puissant qu'une idée dont l'heure est venue* » : le contrôle parlementaire pourra enfin s'exercer sur les services de renseignement.

Je vous remercie, monsieur le préfet.

*

* *

AUDITION DE M. PATRICK CALVAR, DIRECTEUR CENTRAL DU RENSEIGNEMENT INTÉRIEUR

Lors de sa réunion du 30 octobre 2013, la Commission procède à l'audition de M. Patrick Calvar, directeur central du renseignement intérieur.

M. le président Jean-Jacques Urvoas. Nous accueillons aujourd'hui M. Patrick Calvar, directeur central du renseignement intérieur, que je remercie d'avoir répondu à notre invitation.

Si nous avons eu l'occasion, pour certains d'entre nous, de l'entendre à un titre ou à un autre, je tiens à souligner qu'il s'agit de la première fois, sous cette législature comme sous la précédente, que notre commission des Lois auditionne le directeur central du renseignement intérieur, structure qui est aujourd'hui appelée à évoluer et à devenir une direction générale.

Comme pour l'audition de M. le préfet Alain Zabulon, Coordonnateur national du renseignement, la réunion d'aujourd'hui a pour objet de préparer l'examen pour avis par notre Commission, le mercredi 6 novembre prochain, de la loi de programmation militaire, dont M. Patrick Verchère sera le rapporteur pour avis.

Je vous rappelle également que cette audition n'est ni ouverte à la presse, ni retransmise sur Internet. Elle fera, en revanche, l'objet d'un compte rendu public. Je vous demande donc, mes chers collègues, de bien vouloir ne pas « tweeter » les échanges qui vont se tenir au cours de cette réunion.

Je me propose à présent de laisser la parole à M. Patrick Calvar pour qu'il nous présente les missions et le fonctionnement du système français de renseignement intérieur et qu'il évoque les mutations en cours, dont nous avons notamment eu à connaître dans le cadre de la mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, ainsi que de celui de la commission d'enquête sur le fonctionnement de ces mêmes services dans le suivi et la surveillance des mouvements radicaux armés.

À l'issue du propos liminaire de M. Patrick Calvar, je donnerai la parole à notre rapporteur Patrice Verchère puis à ceux et celles d'entre vous qui le souhaiteront pour poser des questions.

M. Patrick Calvar, directeur central du renseignement intérieur. Mesdames, messieurs les députés, c'est en effet la première fois qu'un responsable du renseignement intérieur est entendu par la commission des Lois de l'Assemblée nationale.

Je voudrais, en quelques mots, vous présenter le travail réalisé par la direction centrale du renseignement intérieur (DCRI) ainsi que les objectifs

poursuivis par la création à venir d'une direction générale de la sécurité intérieure. La question sous-jacente est bien celle de savoir si notre pays veut se donner les moyens de se doter d'un service du renseignement intérieur digne de ce nom.

L'actualité récente – et je pense notamment à l'affaire « *Snowden* » – démontre l'utilité – s'il en était encore besoin – de disposer d'un service de cette nature, capable de défendre les intérêts de la France face aux diverses agressions, dont notre pays est victime de manière quotidienne.

L'actuelle DCRI a, en effet, besoin de monter en puissance pour répondre aux deux grandes menaces que sont le terrorisme d'une part, et les atteintes portées à notre souveraineté politique, économique, militaire et diplomatique d'autre part.

Or, pour répondre à ces défis, la DCRI, qui est essentiellement un service de police, doit ouvrir ses portes à d'autres spécialités, telles que l'ingénierie informatique de haut niveau, par exemple, pour faire face aux cyberattaques et accroître sa capacité à recueillir et exploiter le renseignement.

Il est en effet fondamental, pour que la DCRI ait la capacité de protéger les intérêts fondamentaux du pays, que ce service effectue un « saut qualitatif » et dispose de personnels ayant de nouvelles compétences, différentes et complémentaires de celles existant naturellement au sein de la police nationale. Cette tâche n'est pas simple et il convient de faire évoluer les mentalités pour accueillir au sein d'un service « monoculturel » de nouveaux talents, leur permettre d'avoir un véritable déroulement de carrière et ainsi travailler de manière pluridisciplinaire.

Si la priorité est la lutte contre le terrorisme, dont la situation est particulièrement aiguë au regard, par exemple, du nombre de Français qui quittent le territoire pour rejoindre la Syrie, la DCRI lutte également contre l'espionnage, les mouvements radicaux armés, qui cherchent à remettre en cause par la violence la forme républicaine de nos institutions, les proliférations, les cyberattaques et s'efforce de protéger notre patrimoine économique, technologique et scientifique.

L'objet de la loi de programmation militaire, dans son volet relatif au renseignement, est notamment de poser la question des moyens à la disposition des services de renseignement pour mener à bien l'ensemble de ses missions. En l'état actuel du texte, la mesure la plus importante pour nous est celle relative à la géolocalisation, même si d'autres mesures sont aussi notables, comme le droit reconnu aux fonctionnaires du ministère de la Défense d'accéder à certains fichiers et le renforcement des pouvoirs de la délégation parlementaire au renseignement.

Les méthodes de travail évoluant et les menaces changeant de forme, la DCRI doit disposer des moyens nécessaires à l'accomplissement de ses missions. En contrepartie, son action doit s'inscrire dans un système bien défini d'autorisation en amont et de contrôle efficace en aval pour assurer le respect de la

légalité. Pour reprendre l'exemple de l'affaire « Snowden », les fonctionnaires américains ont agi en toute légalité au regard du droit américain et aucun d'eux ne sera poursuivi.

M. le président Jean-Jacques Urvoas. – Je vous remercie, Monsieur le directeur, pour ce propos introductif. Je cède la parole à notre collègue Patrice Verchère

M. Patrice Verchère, rapporteur pour avis. – Monsieur le directeur central – et peut-être directeur général à partir du 1^{er} janvier prochain...

M. Patrick Calvar, directeur central du renseignement intérieur. – Cette nomination relève du président de la République.

M. Patrice Verchère, rapporteur pour avis. – Je me réjouis du succès du rapport d'information que Jean-Jacques Urvoas – probablement le meilleur spécialiste des questions liées au renseignement au sein de notre Assemblée – et moi-même avons publié et dans lequel nous préconisons une évolution de la direction centrale du renseignement intérieur en une direction générale autonome.

Je vais concentrer mes questions sur le projet de loi de programmation militaire.

Ma première question concerne l'anonymat des agents. L'article 27 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, adopté à l'initiative de la précédente majorité mais avec l'appui de l'opposition d'alors, a institué un régime de déposition spécifique aux personnels des services de renseignement qui peuvent être témoins, dans le cadre de leurs missions, de la commission d'une infraction. Malgré ce régime protecteur, on sait que des terroristes ont réussi à établir des listes d'agents, notamment en recoupant des noms figurant dans des procès-verbaux judiciaires. Dans le cadre du projet de loi de programmation militaire, il est proposé de modifier le code de procédure pénale pour que l'audition d'un agent ait lieu dans un lieu « assurant l'anonymat et la confidentialité ». Cette rédaction va-t-elle, de votre point de vue, permettre de garantir effectivement l'anonymat de nos agents ?

Ma deuxième question porte sur le contrôle parlementaire de l'action des services de renseignement. La communauté du renseignement, à l'unanimité, refuse le principe d'une audition d'un agent par la délégation parlementaire au renseignement. Pourtant un sous-amendement du Gouvernement, adopté par le Sénat, propose qu'un directeur de service auditionné par cette délégation puisse être accompagné par le ou les collaborateurs de son choix. Que pensez-vous de cette disposition ? Ne pourrions-nous pas, dans le cadre de la délégation parlementaire au renseignement, aller plus loin et solliciter l'audition d'un agent sans qu'il soit accompagné de son directeur de service, en reprenant, en des termes identiques, la garantie d'anonymat et de confidentialité qui est prévue par le projet de loi pour l'audition d'un agent des services de renseignement par l'autorité

judiciaire ? Si on fait confiance au juge, on devrait pouvoir faire confiance aux parlementaires...

Ma troisième question a trait à la géolocalisation. Le rapport d'information que Jean-Jacques Urvoas et moi-même avons produit a pointé les lacunes en matière de géolocalisation de téléphones mobiles de personnes suspectées de terrorisme. Le dispositif proposé par l'article 13 du projet de loi de programmation militaire répond-il à vos attentes ? Même s'il est renouvelable, un délai maximal de dix jours pour procéder à la géolocalisation en temps réel de suspects vous paraît-il suffisant ?

M. le président Jean-Jacques Urvoas. – Monsieur Calvar, je vais vous laisser répondre d'abord aux questions du rapporteur avant de proposer à nos collègues de vous adresser leurs propres questions.

M. Patrick Calvar, directeur central du renseignement intérieur. – Pour ce qui concerne tout d'abord l'anonymat, la mesure proposée est importante. La loi en vigueur prévoit déjà des poursuites à chaque fois que le nom d'un fonctionnaire des services de renseignement est rendu public. Mais l'application de la loi est battue en brèche : régulièrement, les noms des personnels sont publiés dans la presse. Tout ce qui va dans le sens de la protection de l'identité des agents de renseignement est capital. Nous sommes donc plutôt satisfaits des mesures envisagées.

Même dans un autre contexte, celui de nos activités judiciaires, nous menons actuellement des discussions au sujet de la protection de l'anonymat des agents qui agissent dans le cadre de procédures judiciaires afin d'éviter qu'ils soient identifiés et que leur nom soit publié sur des sites Internet, notamment islamistes, avec tous les risques physiques qui peuvent en découler pour leur personne.

Quant à l'audition de tout agent par la délégation parlementaire au renseignement, il faut garder à l'esprit que, dans un État de droit, tout est question d'équilibre. D'une part, il faut qu'on définisse exactement quelles sont nos possibilités d'action – je rappelle qu'aux États-Unis, dans le cadre de l'affaire « Snowden », les agents américains ont tous agi dans le cadre de la légalité. D'autre part, il faut que l'on réponde des actes accomplis par nos agents.

L'audition de n'importe lequel de ces agents par des parlementaires pourrait cependant avoir des effets pervers.

Tout d'abord, un fonctionnaire, quel que soit son niveau hiérarchique, n'a pas nécessairement une connaissance globale d'un phénomène.

Ensuite, bien des agents des services de renseignement sont peu habitués à être auditionnés par des parlementaires. Si, toutefois, on permettait à la délégation parlementaire au renseignement d'entendre tout agent de ces services, il faudrait envisager une limite : le directeur de service doit pouvoir venir accompagné de la

personne considérée comme la plus qualifiée. Néanmoins, cette précaution n'exclut pas le risque que désormais, tout agent s'auto-inhibe dans son activité quotidienne, ayant conscience qu'il pourrait être un jour auditionné par la délégation parlementaire. Les agents risquent de voir dans cette nouvelle prérogative de la délégation parlementaire un système de contrôle de plus en plus aigu de leur activité, sans pour autant qu'on leur dise clairement dans le même temps ce qu'ils peuvent ou ne peuvent pas faire.

Dans les pays anglo-saxons, les pouvoirs des services de renseignement sont très clairement précisés. Mais je ne suis pas certain que, pour autant, le pouvoir d'audition reconnu aux parlementaires dans ces pays concerne l'ensemble des agents des services de renseignement.

Avant que ne soit votée la disposition étendant le pouvoir d'audition de la délégation parlementaire à tout agent des services de renseignement, il faut mener une réflexion approfondie car les conséquences d'une mesure de cette nature seront fortes. Si, du jour au lendemain, tout fonctionnaire sait qu'il est susceptible d'être entendu par la délégation parlementaire au renseignement, cela risque d'avoir des effets pervers sur le fonctionnement des services et sur la qualité de l'engagement des agents.

Tout est question d'équilibre : si les pouvoirs des services de renseignement sont bien définis, alors le contrôle sur l'exercice de ces pouvoirs peut être poussé.

Il faut avoir conscience que les services fonctionnent selon le principe du « besoin d'en connaître » : chacun d'entre nous est engagé dans une mission dans un cadre précis et ne sait que ce qu'il doit savoir. Les réponses que les agents pourraient apporter à la délégation parlementaire au renseignement pourraient donc être tronquées, faute pour eux d'avoir une vision globale d'une situation. S'il est vrai que la présence à leur côté du directeur de service ayant une vision plus globale peut paraître de nature à pallier cet inconvénient, il n'en reste pas moins qu'il pourrait y avoir des contradictions entre les propos des agents et ceux de leur directeur. L'effet sera alors désastreux. À titre personnel, je suis défavorable à toute mesure qui permettrait à la délégation parlementaire d'entendre n'importe quel agent des services de renseignement. Je conçois cependant que, le cas échéant, un chef de service auditionné par la délégation parlementaire puisse être accompagné par la personne la plus qualifiée pour répondre à un point précis avec la plus grande efficacité et en toute transparence.

Enfin, pour ce qui concerne la géolocalisation, je voudrais tout d'abord rappeler que dans le domaine de la lutte anti-terroriste, nous avons besoin de procéder à des surveillances dans des environnements hostiles. Or il est très difficile de déployer des personnels au sol pendant plusieurs heures au même endroit sans être repéré. Il est donc nécessaire de faire appel à des moyens techniques pour savoir où la personne qui fait l'objet de nos investigations se trouve en temps réel. C'est ce que permet la géolocalisation.

Cette mesure est beaucoup moins intrusive et liberticide que les interceptions des communications dont le régime a été fixé par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

Cette loi reconnaît aux services de renseignement, sur autorisation du Premier ministre après avis de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), le droit d'intercepter pendant quatre mois les communications de personnes faisant l'objet d'investigations. Or, il est proposé de réduire à une période de dix jours le droit reconnu aux mêmes services de procéder à la géolocalisation de suspects, alors qu'il faut au moins un mois pour déterminer la zone d'évolution géographique et l'arborescence relationnelle des personnes surveillées, c'est-à-dire l'univers dans lequel elles évoluent et les individus qu'elles côtoient.

C'est à partir de là que l'on peut mettre en œuvre d'autres moyens de surveillance des personnes faisant l'objet d'investigations : des moyens de surveillance physiques avec le déploiement de personnels au sol, ou techniques.

Compte tenu des méthodes aujourd'hui utilisées par les personnes faisant l'objet d'investigations, il faut bien donner aux services de renseignement les moyens d'agir : je ne comprends pas pourquoi on limiterait le droit de procéder à des géolocalisations à une période de dix jours, alors qu'on autorise des interceptions de communications téléphoniques nettement plus intrusives pendant quatre mois.

M. le président Jean-Jacques Urvoas. – Une durée suffisante pour procéder à des géolocalisations, ce serait donc un mois ?

M. Patrick Calvar, directeur central du renseignement intérieur. – Monsieur le Président, si une période plus longue nous est accordée pour procéder à des géolocalisations, nous y sommes bien sûr favorables.

M. Jean-Frédéric Poisson. Monsieur le directeur central, j'aurais souhaité avoir quelques précisions sur les moyens techniques utilisés dans le cadre d'une opération de géolocalisation.

M. Patrick Calvar, directeur central du renseignement intérieur. Ces moyens sont divers. Nous pouvons demander aux opérateurs téléphoniques et aux fournisseurs d'accès à internet de nous fournir les points d'émission d'un appel ou d'une connexion. Ces techniques nous permettent, lorsqu'elles sont mises en œuvre sur une certaine durée, de mieux connaître l'environnement dans lequel évolue l'objectif.

M. Yann Galut. J'ai conscience que la lutte contre le terrorisme et les cyber-attaques constitue, pour vos services, des priorités que, d'ailleurs, nous partageons. Cependant, vous avez également indiqué avoir pour mission la protection du patrimoine économique de la France. Or, comme vous le savez, la

France est victime d'évasion fiscale, en particulier d'escroqueries à la taxe sur la valeur ajoutée (TVA). Cette forme de fraude fiscale est assurément liée à l'activité de réseaux criminels qui, pour certains, seraient également susceptibles de financer des activités terroristes. Le « carrousel TVA » coûte à la France, chaque année, environ 10 milliards d'euros. La Commission européenne a même évalué cette perte de recettes fiscales à 32 milliards d'euros par an pour la France. Ce phénomène s'est d'ailleurs amplifié ces dernières années. Or, je suppose que la DCRI dispose d'informations sur ces réseaux mafieux. Dès lors, ma question est la suivante : avez-vous, au-delà des priorités absolues qui sont les vôtres, engagé une réflexion sur ce phénomène qui n'est pas tout à fait étranger à vos préoccupations ?

M. Patrick Calvar, directeur central du renseignement intérieur. Il existe désormais une communauté du renseignement, composée de six services : la direction générale de la sécurité extérieure (DGSE) et la DCRI, deux services à vocation généraliste ; les services du ministère des Finances que sont la direction nationale du renseignement et des enquêtes douanières (DNRED) et Tracfin ; enfin, les services rattachés au ministère de la Défense, la direction du renseignement militaire (DRM) et la direction de la protection et de la sécurité de la défense (DPSD).

La lutte contre la fraude fiscale ne constitue pas, aujourd'hui, l'une de nos missions. Cependant, dans le cadre de la création de la direction générale de la sécurité intérieure, nous conduisons une réflexion sur l'opportunité de nous impliquer dans la lutte contre la criminalité organisée dès lors qu'elle vise nos intérêts stratégiques, par exemple en cas de blanchiment, de prise de participation dans des sociétés ou d'attaque du réseau bancaire ou énergétique. Pour l'heure, notre rôle se borne à transmettre aux services compétents les informations de cette nature qui peuvent entrer en notre possession.

Si la DCRI devait lutter contre la fraude fiscale, il faudrait considérablement renforcer ses pouvoirs ; car elle aurait alors à faire face à des acteurs puissants, bénéficiant de structures juridiques de défense solides. À l'heure actuelle, la DCRI n'a pas accès aux données bancaires ; une loi serait indispensable pour que le secret bancaire ne soit plus opposable à la DCRI. Mais cela suppose, d'une part, une volonté politique et, d'autre part, des moyens humains – notamment des analystes financiers chevronnés –, financiers et juridiques spécifiques.

M. le président Jean-Jacques Urvoas. La Cour des comptes a d'ailleurs récemment indiqué que la lutte contre la fraude fiscale devrait s'appuyer sur la DCRI.

Mme Marie-Françoise Bechtel. Sur la question de la lutte contre la fraude fiscale, il me semblerait préjudiciable, dans le monde dangereux qui est le nôtre, de confier à un même service des missions d'une telle diversité. Monsieur le directeur central, je partage par ailleurs votre point de vue concernant l'audition éventuelle de vos agents par la délégation parlementaire au renseignement. Il ne

faut pas que de telles auditions conduisent à des informations tronquées et ce qu'on peut qualifier de « centralisation du dialogue » au travers des chefs des services me paraît nécessaire.

Je souhaiterais vous soumettre deux questions. D'une part, à l'occasion de l'examen du projet de loi relatif à la sécurité et à la lutte contre le terrorisme, en 2012, nous nous étions interrogés sur l'opportunité d'autoriser l'espionnage actif des réseaux informatiques, c'est-à-dire le fait, pour un agent, de pénétrer un réseau et d'engager un dialogue avec les terroristes qui y participent. Pour des raisons constitutionnelles, nous n'avions pas examiné ces dispositions. Pensez-vous qu'il soit nécessaire de donner ce pouvoir aux services de renseignement ?

D'autre part, la lutte antiterroriste semble de plus en plus fréquemment servir de prétexte à un espionnage économique de la part de pays alliés. Ces pratiques, qui ont toujours existé, semblent aujourd'hui être massives, comme le suggère l'affaire des écoutes américaines, et s'appuient vraisemblablement sur des technologies très avancées. À votre avis, la mise en place d'un bouclier numérique est-elle envisageable, afin de contrer toute tentative d'espionnage et, en particulier, ces écoutes massives de la part de pays alliés ?

M. Patrick Calvar, directeur central du renseignement extérieur. Pour répondre à votre première question, il existe à l'évidence une nécessité absolue de se doter de moyens performants de surveillance de l'Internet, qui est aujourd'hui au cœur des entreprises terroristes, des actions prosélytes, des processus de recrutements et du montage d'opérations aboutissant *in fine* à des actions violentes. Des réflexions sont en cours pour déterminer les moyens de progresser en la matière, mais on ne peut en rester à une réflexion hexagonale. Un approfondissement de la coopération internationale est nécessaire, car il s'agit le plus souvent de surveiller des serveurs situés hors de notre territoire. La réflexion doit, au-delà de notre pays, être européenne, et même étendue à d'autres pays. Nous devons aussi réfléchir à la création de nouvelles incriminations pénales, afin notamment de mieux poursuivre les administrateurs des sites en question. Aujourd'hui, les infractions à la loi sur la presse, qu'il s'agisse d'incitations à la commission d'actes ou d'apologie d'actes terroristes ne suffisent pas à engager de telles poursuites ; nous parvenons tout au plus, dans certaines affaires, à engager des poursuites sur le fondement de l'association de malfaiteurs en lien avec une entreprise terroriste, dès lors que les personnes mises en cause ont commis des actes positifs, par exemple l'envoi d'agents sur des zones de *Djihad*.

S'agissant des dérives que vous évoquiez, relatives à l'utilisation des moyens de surveillance d'Internet aux fins d'intelligence économique, je crois que notre pays n'a pas assez pris conscience des dangers que représente l'Internet. Les pouvoirs publics doivent mener une réflexion d'ensemble sur cette question, en s'appuyant sur les organismes existants afin d'inciter les entreprises françaises à engager des démarches d'autoprotection. La sécurité n'est pas une chose naturelle chez nos compatriotes. Nos entreprises n'ont pas la culture qu'ont les entreprises anglo-saxonnes en la matière. Or, la révolution numérique nous montre à quel

point le danger est à nos portes, et même a franchi nos portes. C'est un des enjeux majeurs de demain. Nous souhaitons nous doter d'une capacité de lutte, mais cette capacité ne sera pas suffisante, donc il faut, dans le cadre de la communauté du renseignement, que nos services s'intègrent à d'autres, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il faut aller plus loin, au travers de l'éducation, pour modifier les comportements, dans une logique sécuritaire.

Enfin, tant que l'Europe ne sera pas dotée d'opérateurs puissants, elle restera en situation de très grande faiblesse. Il faut avoir conscience du fait que toutes les entreprises américaines ont passé des accords avec l'État américain. Quand on songe aux grandes entreprises européennes de téléphonie, et à leur perte de vitesse par rapport à leurs concurrents, notamment américains, on voit bien que la situation est différente. Les États européens restent dépendants, alors même que l'Europe demeure la première puissance économique mondiale.

M. Dominique Raimbourg. Pardonnez ma question de néophyte, mais lorsque vous comparez tout à l'heure les techniques d'écoutes téléphoniques et de géolocalisation, vous n'avez pas mentionné les questions de procédures d'autorisation dans le cadre administratif ; si elles étaient rendues identiques, c'est-à-dire, si le recours à la géolocalisation était soumis au contrôle préalable d'une commission indépendante, sans doute cela n'autoriserait-il pas un alignement des durées maximales autorisées ?

M. Patrick Calvar, directeur central du renseignement intérieur. Le projet de loi de programmation militaire instaure, pour la géolocalisation, une procédure analogue à celle qui existe pour les interceptions de sécurité avec un contrôle exercé par la Commission nationale de contrôle des interceptions de sécurité. Si vous souhaitez mon avis sur la question de la durée de l'autorisation, je vous dirai que plus elle est longue, plus les renseignements que les services pourront en retirer seront riches et utiles. À ce sujet, je souhaite vraiment insister sur le fait que les personnes que nous surveillons sont extrêmement mobiles et méfiantes. La clandestinité est le mode de vie des terroristes. Ils se cachent dans des lieux très difficiles à surveiller et parlent très peu par téléphone, ce qui rend notre surveillance de plus en plus délicate. Dans ces conditions, nos services ont besoin de nouveaux dispositifs techniques d'intrusion, au risque, sinon, d'amoindrir très fortement notre capacité à les surveiller.

En matière de lutte contre le terrorisme, nous ne manquons pas d'informations, qui circulent très rapidement au plan international, sans barrières. Nos services ne pâtissent pas d'une absence de coopération entre les États ; bien au contraire, nous recevons une masse très importante d'informations et l'enjeu crucial pour nous réside dans le choix qu'il faut opérer pour concentrer nos capacités d'analyse sur certaines plutôt que sur d'autres. Or, ces choix sont difficiles et peuvent s'avérer erronés, avec des conséquences potentiellement dramatiques.

D'ailleurs, nos services se retrouvent dans une situation proche de la schizophrénie, lorsqu'ils doivent tout à la fois utiliser les informations transmises par les grands services étrangers, notamment en matière de lutte contre le terrorisme, tout en se méfiant par ailleurs de la capacité de ces mêmes services à exercer une surveillance et à attaquer la souveraineté de notre pays.

Mme Françoise Descamps–Crosnier. Vous avez déjà en partie répondu aux questions que je souhaitais vous poser. Lors de votre audition par la commission de la Défense nationale et des forces armées de l'Assemblée nationale le 26 février dernier, vous avez déclaré : « *Un autre défi tient à ce que nous avons affaire à de nouveaux adversaires aux méthodes très inventives, alors que nous en sommes restés à des moyens d'action presque archaïques* ». Vous évoquiez les écoutes téléphoniques qui « *n'ont plus aucun intérêt* » et vous disiez : « *d'ailleurs, tout passe désormais par l'Internet, mais de quels moyens de surveillance de l'Internet disposons-nous ?* ». Vous évoquiez, bien sûr, le cadre judiciaire, en citant certaines techniques, mais en soulignant qu'« *aucune de ces techniques n'est autorisée en renseignement* ». Dès lors, comment parvenez-vous à mener une lutte performante contre les réseaux ?

Confrontés à la révélation de l'affaire d'espionnage par la NSA, nous devons nous interroger sur les failles de notre système : avons-nous les moyens de faire face à une cyberattaque et à défendre notre souveraineté ? Avez-vous estimé nos besoins en la matière ? Comment, selon vous, le législateur peut-il faire évoluer les textes pour réduire la contrainte légale qui freine l'action de vos services ? Quelle est votre position sur une éventuelle loi-cadre sur le renseignement qu'appelait de ses vœux votre prédécesseur dans une interview récente ?

M. Patrick Calvar, directeur central du renseignement intérieur. Comment faire ? Nous voyons que la technique évolue beaucoup plus vite que le droit. La puissance des systèmes d'interception américains est telle qu'ils sont de moins en moins contrôlés par l'homme, et de plus en plus par la machine elle-même. De notre côté, nous avons une obligation de résultat dans la lutte anti-terroriste : c'est pourquoi nous avons besoin, d'une part, que l'on nous dise clairement ce que nous pouvons faire et entreprendre, et, d'autre part, d'un « contrepoids ». Ce que nous faisons est légitime et nous devons être confortés dans notre action. Je comprends aussi bien évidemment la sensibilité de l'opinion publique sur ces sujets.

Nous sommes pris, avec les Américains, dans un conflit asymétrique : contrairement aux leurs, nos filières universitaires n'ont pas encore vraiment promu d'enseignement ou de recherche sur la sécurité informatique ; or les entreprises ont besoin de se protéger, et c'est d'ailleurs le rôle de l'État de protéger l'économie nationale. Pourtant, nous prenons du retard, et si l'on aborde la question sous l'angle du droit, on constate que le droit ne comprend pas la technique.

M. le président Jean-Jacques Urvoas. Que répondez-vous à la suggestion de M. Squarcini relative à la nécessité d'une loi-cadre sur le renseignement ?

M. Patrick Calvar, directeur central du renseignement intérieur. Je trouve l'approche anglo-saxonne très pragmatique. S'en inspirer permettrait d'avoir des règles claires quant à nos possibilités légales d'action, puis le contrôle *a posteriori* permet de vérifier si les actes effectués respectaient bien le cadre légal. Or, nous sommes dans une « zone grise » qui rend l'action difficile. Nous avons besoin de missions définies, de moyens adaptés, de pouvoirs juridiquement reconnus et de contrôles.

M. Patrice Verchère, rapporteur pour avis. Quel est votre avis quant à la nécessité de disposer d'un système de données des dossiers passagers (*PNR* ou *Passenger Name Record*) au niveau de l'Union européenne ?

M. Patrick Calvar, directeur central du renseignement intérieur. Le *PNR* national tel qu'il est actuellement discuté dans la loi de programmation militaire est une avancée. Mais un *PNR* « européen » me paraîtrait très positif, car on se prive d'un outil très utile en l'absence de cette source d'information au niveau communautaire. Je rappelle par ailleurs que nous avons donné aux Américains de très importantes données financières dans le cadre de l'accord *SWIFT*, et que nous répondons à leurs exigences de transmissions d'information dans le cadre de leur propre *PNR*, alors que nous n'y avons pas nous-mêmes accès !

M. le président Jean-Jacques Urvoas. Lors de sa première audition par la Commission des Lois, en juillet 2012, le ministre de l'Intérieur, M. Manuel Valls, avait évoqué des failles observées dans l'affaire Merah. Avec le recul, quelles conclusions tirez-vous non pas sur cette affaire précise, mais quant au fonctionnement de nos services de renseignement ?

Les relations de votre service, qui dispose de « représentations » hors de nos frontières, avec les services étrangers ont-elles connu des évolutions à la suite des révélations du journal *Le Monde* et de l'affaire Snowden ?

Enfin quand s'effectuera la transformation de votre service en direction générale de la sécurité intérieure (DGSI) ? La date du 1^{er} janvier 2014 a été évoquée.

M. Patrick Calvar, directeur central du renseignement intérieur. À votre première question je répondrai qu'aucun service n'est infaillible et que l'on peut connaître des échecs. Une instruction judiciaire étant en cours, je ne peux naturellement m'exprimer sur le fond du dossier Merah. Nous sommes obligés de définir des priorités. Nous avons besoin de professionnaliser nos fonctionnaires et de développer nos capacités d'analyse.

Nous avons besoin d'étoffer nos effectifs avec de nouveaux talents. Des

erreurs sont toujours possibles ; il faut en avoir conscience. D'ailleurs, dans certaines affaires nous avons heureusement échappé de peu à des conséquences très graves : ainsi l'affaire de la grenade jetée dans une épicerie à Sarcelles, qui aurait pu faire des victimes, ou le soldat qui a été poignardé à La Défense. Dans le cas de Sarcelles, on s'est aperçu après coup que l'auteur était connu de nos services.

Il existe actuellement beaucoup de profils différents de personnes qui peuvent commettre des actes violents, dont des cas qui touchent à la psychiatrie. Des filières très organisées agissent sur le long terme. Beaucoup de jeunes partent également en ce moment en Syrie, où ils évoluent dans un univers de guerre totale atroce, et l'on peut craindre l'état d'esprit dans lequel ils reviendront en France. Il y a enfin des personnes qui contestent violemment notre société, et qui peuvent passer à l'acte. Il nous faut aussi gérer la dimension médiatique : quelqu'un qui tue en se réclamant d'Al-Qaïda bénéficiera immédiatement d'un grand retentissement médiatique.

S'agissant, ensuite, des liens entretenus par la DCRI avec ses interlocuteurs étrangers, je rappellerai que l'objectif de ces liens est de coopérer avec les services de renseignement étrangers, à la différence des activités de la DGSE à l'étranger qui ont pour objet la recherche d'informations. En pratique, la DCRI a des échanges avec plusieurs dizaines de partenaires étrangers.

La relation avec le partenaire américain est une relation asymétrique : d'un côté, on ne peut pas se passer de la relation avec les services américains – comme l'a, du reste, montré l'affaire Merah, puisque la NSA l'avait localisé au Pakistan – mais, de l'autre côté, il n'est pas acceptable que ce partenaire continue à procéder comme il le fait à notre égard. Sachant que les révélations faites par le quotidien *Le Monde* sur les écoutes pratiquées par la NSA n'en sont vraisemblablement qu'à leur début, il est nécessaire de marquer un coup d'arrêt à ces pratiques.

M. le président Jean-Jacques Urvoas. Les révélations du journal *Le Monde* ont-elles entraîné un « rafraîchissement » des relations avec les États-Unis ?

M. Patrick Calvar, directeur central du renseignement intérieur. La coopération se poursuit en matière de lutte contre le terrorisme, mais la question peut se poser sur d'autres sujets.

Enfin, s'agissant de votre dernière question, monsieur le président, sur la date de création de la direction générale de la sécurité intérieure, il ne serait pas raisonnable de l'envisager avant la fin du premier trimestre 2014. En effet, cette création nécessite de réviser de nombreux textes, de répondre à certaines interrogations relatives au statut des fonctionnaires, de définir précisément ses missions et, enfin, de régler les questions budgétaires.

M. le président Jean-Jacques Urvoas. Monsieur le directeur, je vous remercie pour vos réponses.

EXAMEN DES ARTICLES

Lors de sa réunion du mercredi 6 novembre 2013, la Commission examine pour avis, sur le rapport de M. Patrice Verchère, le projet de loi, adopté par le Sénat, relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (n° 1473).

Après l'exposé du rapporteur pour avis, la Commission passe à l'examen des articles du projet de loi dont elle s'est saisie pour avis.

CHAPITRE I^{ER} BIS

Dispositions relatives au contrôle parlementaire de l'exécution de la loi de programmation

Le présent chapitre, qui compte quatre articles, a été inséré par la commission des Affaires étrangères, de la défense et des forces armées du Sénat, qui a estimé qu'il convenait de renforcer les dispositions relatives au contrôle parlementaire de l'exécution des lois de programmation.

Article 4 ter

Contrôle sur pièces et sur place pour les membres des commissions parlementaires chargées de la défense

Le présent article, introduit par un amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, a pour objet de conférer aux rapporteurs pour avis sur le projet de loi de finances ainsi qu'à des membres spécialement désignés à cet effet par les commissions chargées de la défense des deux assemblées, des pouvoirs identiques à ceux dont disposent les rapporteurs spéciaux des commissions des Finances et ce, aux fins de « *suivre et contrôler* » l'application de la loi de programmation militaire.

Le second alinéa de cet article prévoit que le ministère de la Défense devra leur transmettre tous renseignements et documents d'ordre financier et administratif utiles à l'exercice de leur mission, dans le respect toutefois du secret de la défense nationale.

En application du IV de l'article 164 de l'ordonnance n° 58-1374 du 30 décembre 1958 portant loi de finances pour 1959⁽¹⁾, le président, le rapporteur général et les rapporteurs spéciaux des commissions chargées des finances, dans leurs domaines d'attribution, « *suivent et contrôlent de façon permanente, sur pièces et sur place, l'exécution des lois de finances, l'emploi des crédits, l'évolution des recettes de l'État et de l'ensemble des recettes publiques affectées* ». Ce même article prévoit que « *tous les renseignements d'ordre*

(1) Toujours en vigueur, malgré la reprise de certaines de ces dispositions par la loi organique n° 2001-692 du 1^{er} août 2001 relative aux lois de finances (LOLF).

financier et administratif de nature à faciliter leur mission doivent être fournis », réserve faite, d'une part, des « *sujets de caractère secret concernant la défense nationale, les affaires étrangères, la sécurité intérieure ou extérieure de l'État* » et, d'autre part, « *du principe de la séparation du pouvoir judiciaire et des autres pouvoirs* ».

Les pouvoirs propres au président, au rapporteur général et aux rapporteurs spéciaux de la commission des Finances ont été renforcés – et élevés au niveau organique – par la LOLF, dont l'article 57 prévoit qu'ils « *suivent et contrôlent l'exécution des lois de finances et procèdent à l'évaluation de toute question relative aux finances publiques* ». À cet effet, « *ils procèdent à toutes investigations sur pièces et sur place, et à toutes auditions qu'ils jugent utiles* ».

Le présent article propose donc d'étendre au cas de l'application des lois de programmation militaire des dispositions prévue par l'ordonnance du 30 décembre 1958 – non organique – et par la LOLF – organique.

Ce faisant, le présent article crée une ambiguïté sur la nature du contrôle que les commissions chargées de la défense exerceraient. En matière budgétaire, c'est sur un fondement organique que repose la compétence des commissions chargées des finances. Mais, en dehors du contrôle de l'emploi des deniers publics, le législateur peut tout-à-fait prévoir que certains organes parlementaires disposent de pouvoirs spécifiques. Il en est ainsi :

— des commissions d'enquête, pour lesquelles l'article 6 de l'ordonnance (non organique) n° 58-1100 du 17 décembre 1958 relative au fonctionnement des assemblées parlementaires prévoit des pouvoirs de contrôle « *sur pièces et sur place* » pour leurs rapporteurs ;

— du Comité d'évaluation et de contrôle des politiques publiques (de l'Assemblée nationale) ou d'autres instances de contrôle y compris des commissions permanentes, pour lesquels l'article 5 *ter* de l'ordonnance du 17 décembre 1958 précitée prévoit qu'ils peuvent « *demander à l'assemblée à laquelle elles appartiennent, pour une mission déterminée et une durée n'excédant pas six mois, de leur conférer, dans les conditions et limites prévues par cet article, les prérogatives attribuées aux commissions d'enquête* »

Le présent article ne porte pas, en tant que tel sur le contrôle de l'emploi des deniers publics mais confère des pouvoirs de contrôle sur pièces et sur place à des « *rapporteurs budgétaires* ». Il convient d'ailleurs de noter que cette notion de « *rapporteurs budgétaires* » n'est pas définie juridiquement et qu'elle doit être entendue comme renvoyant aux rapporteurs pour avis sur le projet de loi de finances, désignés par les commissions chargées de la défense.

En outre, il faut observer que le présent article ne précise pas clairement que les pouvoirs conférés aux commissions chargées de la défense sont limités par le secret de la défense nationale. Dès 1958, les pouvoirs de contrôle dévolus à la commission des Finances ont été limités par ce secret – à l'instar d'ailleurs de

toutes les instances parlementaires à l'exclusion de la délégation parlementaire au renseignement.

Le dispositif adopté par le Sénat mériterait donc certainement des clarifications. En effet, il ne précise que dans son second alinéa, relatif à la transmission, par le ministre de la défense, de renseignements et de document, que cette transmission s'effectue « *dans le respect du secret de la défense nationale* », sans que cette même précision ne figure à l'alinéa précédent qui fixe les pouvoirs de contrôle des commissions chargées de la défense.

En conséquence, les pouvoirs de contrôle « *sur pièces et sur place* » des commissions chargées de la défense ne semblent pas, en l'état, limités par le respect du secret de la défense nationale. En application de cet alinéa, ces commissions pourraient donc exercer un contrôle identique à celui de la délégation parlementaire au renseignement, voire d'ailleurs, un contrôle encore plus large que celui de cet organe puisque portant sur l'ensemble du ministère de la Défense et de ses activités et non uniquement sur les éléments relevant du renseignement.

Enfin, les pouvoirs du président, du rapporteur général et des rapporteurs spéciaux des commissions chargées des finances ont fait l'objet d'améliorations pour en asseoir l'effectivité. C'est ainsi que le législateur a prévu, par l'article 31 de la loi de finances rectificative pour 2000 (n° 2000-656 du 13 juillet 2000)⁽¹⁾ que le « *fait de faire obstacle, de quelque façon que ce soit, à l'exercice des pouvoirs d'investigation* » des membres des commissions chargées des finances est puni de 15 000 euros d'amende. Ce même article permet, en outre, au président de l'assemblée concernée, ou au président de la commission des Finances concernée de « *saisir le parquet près la juridiction compétente en vue de déclencher l'action publique* ». L'effectivité de ces pouvoirs a encore été renforcée par la LOLF, dont l'article 59 prévoit que les présidents des commissions chargées des finances « *peuvent demander à la juridiction compétente, statuant en référé, de faire cesser cette entrave [aux prérogatives de contrôle sur pièces et sur place] sous astreinte* ».

Votre rapporteur pour avis observe que le dispositif adopté par le Sénat n'est assorti d'aucun dispositif de cette nature, visant à en assurer l'effectivité.

*

* *

M. le président Jean-Jacques Urvoas. Bien que je ne sois saisi d'aucun amendement sur cet article, je voudrais revenir sur ce qu'a dit le rapporteur.

En l'état, le texte prévoit que les commissions de l'Assemblée nationale et

(1) Cette loi a complété le IV de de l'article 164 de l'ordonnance n° 58-1374 du 30 décembre 1958 portant loi de finances pour 1959.

du Sénat chargées de la défense seront dotées de pouvoirs d’investigation sur pièces et sur place comparables à ceux dont disposent les rapporteurs spéciaux des commissions des Finances. Je comprends l’intention, qui est de contrôler la bonne application de la loi de programmation militaire ; toutefois, je suis sceptique quant au moyen législatif utilisé, car les pouvoirs spéciaux des rapporteurs des commissions des Finances trouvent leur origine, non dans une loi ordinaire, mais dans une loi organique. J’alerte les collègues de la commission de la Défense : il faut qu’ils examinent ce point avec attention.

La Commission émet un avis favorable à l’adoption de l’article 4 ter sans modification.

Article 4 quater

Réunions de contrôle de l’exécution de la loi de programmation

Le présent article, introduit par un amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, dispose que chaque semestre, le ministre de la Défense présente aux commissions permanentes de l’Assemblée nationale et du Sénat un bilan qualifié de « détaillé » de l’exécution de la loi de finances et de la présente loi de programmation.

Ainsi, vise-t-il à consacrer au niveau législatif les réunions de contrôle du budget de la défense, qui réunissent aujourd’hui, chaque semestre, au ministère de la Défense, les représentants du ministère de la Défense et les députés et sénateurs, les présidents et rapporteurs spéciaux de la commission des Finances et les présidents et les rapporteurs budgétaires membres des commissions chargées de la défense de l’Assemblée nationale et du Sénat.

On peut s’étonner de la teneur de cet article qui semble « obliger » le ministre à rendre compte à une commission parlementaire à échéances précises et de manière détaillée. Dans la mesure où cet article impose au ministre de « présenter » ce bilan, on peut l’interpréter comme l’enjoignant de venir physiquement s’exprimer devant les commissions chargées de la défense. Un tel dispositif va au-delà de ce qui est aujourd’hui prévu par l’alinéa 1 de l’article 45 du Règlement de l’Assemblée nationale qui dispose que « [l]es ministres ont accès dans les commissions » et qu’« ils doivent être entendus quand ils le demandent ». L’alinéa 2 du même article ajoute que le bureau de chaque commission « peut » demander l’audition d’un membre du Gouvernement. Il n’est donc pas prévu que le ministre ait l’obligation de déférer à une telle demande et ce, en application du principe de séparation des pouvoirs.

*

* *

La Commission émet un avis favorable à l’adoption de l’article 4 quater sans modification.

Article 4 quinquies

(art. L. 143-5 du code des juridictions financières)

Transmission des observations de la Cour des comptes aux commissions chargées de la défense et des affaires étrangères

Le présent article, introduit par un amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, a été réécrit par un amendement de sa commission des Lois adopté en séance publique.

En premier lieu – et c’était l’objet de l’amendement de la commission des Affaires étrangères – le présent article prévoit, dans son 1^o, que les communications de la Cour des comptes aux ministres et les réponses qui leur sont apportées sont transmises non seulement – comme c’est aujourd’hui le cas en application du principe d’assistance de la Cour des comptes au Parlement prévu par l’article 58 de la loi organique relative aux lois de finances et de l’article L.O. 113-1 du code de la sécurité sociale, issu de la loi organique relative aux lois de financement de la sécurité sociale – aux commissions des Finances et, dans leur domaine de compétence, aux commissions chargées des affaires sociales de chacune des assemblées parlementaires, mais également désormais aux commissions chargées « *de la défense et des forces armées et des affaires étrangères* ».

Votre rapporteur pour avis estime qu’il n’y a aucune raison de limiter aux seules commissions chargées de la défense et des affaires étrangères la transmission des communications de la Cour des comptes, car d’autres commissions permanentes peuvent aussi tirer profit de ces communications dans le cadre de leurs fonctions de contrôle. Aucune disposition constitutionnelle ou organique – à l’instar de ce qui est prévu dans le cadre du projet de loi de finances ou au projet de loi de financement de la sécurité sociale – ne donne de fondement à ce traitement spécifique.

La Commission a donc adopté un amendement de votre rapporteur pour permettre à toutes les commissions permanentes du Parlement de bénéficier de l’expertise de la Cour des comptes.

En second lieu – c’était l’apport de la commission des Lois du Sénat – le présent article prévoit, dans son 2^o, la transmission par le Gouvernement à la délégation parlementaire au renseignement des communications de la Cour des comptes aux ministres portant sur les services de renseignement, ainsi que les réponses qui leur sont apportées.

*

* *

La Commission est saisie de l’amendement CLI du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Il n'y a aucune raison de limiter la transmission des communications de la Cour des comptes aux seules commissions chargées de la défense et des affaires étrangères. Cet amendement vise à permettre à toutes les commissions permanentes de bénéficier de cette expertise.

La Commission adopte l'amendement.

La Commission émet un avis favorable à l'adoption de l'article 4 quinquies ainsi modifié.

Article 4 sexies

Rapport et débat au Parlement sur le contrôle de l'exécution des lois de programmation et diverses autres mesures

Le présent article, introduit par un amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, vise à prévoir un débat annuel au Parlement sur l'exécution de la présente loi de programmation militaire. Ce même article précise que ce rapport contient « *la stratégie d'acquisition* » des équipements militaires, qui définit les « *grandes orientations en matière de systèmes d'armes* ». En outre, ce rapport devra contenir une partie relative au suivi de l'exécution du plan d'accompagnement économique des territoires affectés par des restructurations.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 4 sexies sans modification.

CHAPITRE II

Dispositions relatives au renseignement

Article 5

(art. 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958)

Renforcement des prérogatives de la délégation parlementaire au renseignement

Le présent article vise à renforcer les prérogatives de la délégation parlementaire au renseignement.

Cette délégation a été instituée par la loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement. Comme le rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement⁽¹⁾ l'a montré, la France était, avant 2007, l'une des rares

(1) MM. Jean-Jacques Urvoas et Patrice Verchère, Pour un « État secret » au service de notre démocratie, rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, doc. AN n° 1022, 14 mai 2013.

démocraties occidentales à ne pas disposer d'un organe parlementaire chargé spécifiquement du contrôle des services de renseignements. Il n'existait que des contacts ponctuels entre les commissions compétentes du Parlement et les services de renseignement, par exemple lors de l'examen du budget.

Votre rapporteur estimait d'ailleurs que « *le principal apport de la [délégation parlementaire au renseignement] a précisément été de permettre à une fragile confiance de s'instaurer entre les services de renseignement et la représentation nationale* » et que loin de constituer « *un contrôle parlementaire efficace, la délégation doit être considérée comme l'aboutissement timide d'un effort de plus de quarante années pour établir un droit de regard sur ces administrations* »⁽¹⁾.

Rappelons que la délégation, qui est un organe commun à l'Assemblée nationale et au Sénat, est composée de huit membres, quatre députés et quatre sénateurs. Parmi ces huit membres, quatre sont membres de droit – il s'agit des présidents des commissions en charge de la sécurité intérieure – les commissions des Lois – et des commissions chargées de la défense des deux assemblées – et quatre membres sont nommés par les présidents des assemblées, avec obligation de garantir la présence de l'opposition. La présidence de la délégation est assurée par un membre de droit issu alternativement de l'Assemblée nationale et du Sénat, qui change tous les ans.

La loi attribue à la délégation un rôle plus global que celui dévolu aux autres organes de contrôle parlementaires. Ce rôle est d'ailleurs défini en des termes assez généraux : la délégation « *a pour mission de suivre l'activité générale et les moyens des services spécialisés* » qui relèvent des ministères de la Défense, de l'Intérieur et des Finances. La loi prévoit que dans le cadre de ses fonctions, elle est uniquement informée des éléments relatifs « *au budget, à l'activité générale et à l'organisation des services* ». Le texte prend en outre la précaution d'interdire explicitement la transmission à la délégation de tout élément relatif :

– aux activités opérationnelles des services et aux instructions données par les pouvoirs publics à cet égard. Il convient de souligner que si l'impossibilité de connaître des activités opérationnelles découle de la jurisprudence du Conseil constitutionnel, la question des instructions paraît en revanche plus sujette à caution ;

– au financement des activités opérationnelles, mission dévolue à la commission de vérification des fonds spéciaux ;

– aux échanges avec des services étrangers ou des organismes internationaux compétents dans le domaine du renseignement. Cette précision semblait indispensable pour garantir la protection de l'une des lois d'airain du renseignement, la règle du « *tiers de confiance* » : toute donnée transmise par un

(1) Ibid., p. 76.

service à une instance partenaire reste la propriété du premier. Ainsi l'organe qui en a bénéficié ne peut en aucun cas la diffuser auprès d'un tiers, y compris dans le cadre d'une procédure judiciaire, sans autorisation préalable de son propriétaire.

Pour compléter son information, la délégation peut entendre le Premier ministre, les ministres compétents ainsi que le secrétaire général de la défense et de la sécurité nationale. S'agissant des agents eux-mêmes, seuls les directeurs de service en fonction peuvent être auditionnés, ce qui exclut les subordonnés et les anciens responsables.

Les missions et l'activité de la DPR sont donc strictement bornées et c'est à dessein que le terme de contrôle n'apparaît pas dans le texte, comme l'expliquait le rapporteur du projet de loi, M. Bernard Carayon : « *Le terme de « contrôle » n'est volontairement pas utilisé dans le projet de loi, celui-ci ayant une connotation trop intrusive. Cette absence pourra être critiquée, mais elle est probablement nécessaire pour permettre la mise en place progressive de l'indispensable climat de confiance mutuelle* » ⁽¹⁾.

Pour autant, la délégation a su nouer des rapports de confiance avec les services, ce qui a lui a permis d'obtenir, dans les faits, plus d'informations que ce que la loi prévoit actuellement.

Le présent article propose plusieurs dispositions tenant à renforcer les prérogatives de la délégation parlementaire au renseignement.

La délégation parlementaire au renseignement se verrait reconnaître la mission générale du « *contrôle parlementaire de l'action du Gouvernement en matière de renseignement* » et de l'évaluation de la politique publique en ce domaine.

Dans la version initiale du présent projet de loi, la délégation parlementaire au renseignement aurait été « *informée de la stratégie nationale du renseignement et du plan national d'orientation du renseignement* ». Le Sénat a précisé, sur l'initiative de sa commission des Lois et avec l'accord du Gouvernement, que la stratégie nationale du renseignement lui sera « *transmise* » et qu'elle pourra « *prendre connaissance* » du plan national d'orientation du renseignement.

Par ailleurs, un rapport annuel de synthèse des crédits du renseignement et un rapport annuel d'activité de la communauté française du renseignement lui seraient également présentés.

Votre Commission a précisé, en adoptant un amendement de votre rapporteur pour avis, que le Premier ministre communique à la délégation « des éléments d'information » issus du plan national d'orientation du renseignement,

(1) Bernard Carayon, *Rapport fait au nom de la Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n° 13), adopté par le Sénat, portant création d'une délégation parlementaire au renseignement, doc. AN n° 83, 18 juillet 2007, p. 26.*

plutôt que le plan lui-même afin d'éviter qu'un autre document ne soit élaboré dans le seul but de ne pas communiquer certaines informations aux parlementaires.

Par un autre amendement de la commission des Lois, le Sénat a précisé, avec l'accord du Gouvernement, que la délégation serait « *destinataire des informations utiles à l'accomplissement de sa mission* », dans le souci d'ouvrir à la délégation un accès plus large aux diverses sources d'information disponibles.

S'agissant des « *informations et des éléments d'appréciation relatifs au budget, à l'activité générale et à l'organisation des services de renseignement* » que le Gouvernement peut transmettre à la délégation, le Sénat a précisé qu'ils pouvaient porter sur « *des activités opérationnelles de ces services, les instructions données par les pouvoirs publics à cet égard et le financement de ces activités* » et ce, sauf opposition motivée du Premier ministre. Cette rédaction s'inspire de la décision du Conseil constitutionnel n° 2001-456 DC du 27 décembre 2001 ⁽¹⁾ dans laquelle il a estimé que le Parlement ne saurait intervenir dans les « *opérations en cours* ». Le Gouvernement s'est déclaré favorable à cet amendement, sous réserve que le refus du Premier ministre à la transmission de ces informations n'ait pas à être motivé. Il a présenté un sous-amendement en ce sens, que le Sénat a adopté.

L'amendement adopté par votre Commission précise que les informations transmises ne peuvent porter ni sur les opérations en cours de ces services (reprenant ainsi les termes de la jurisprudence du Conseil constitutionnel précitée), ni sur les instructions données par les pouvoirs publics à cet égard, ni sur les échanges avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement. Ces précisions figurent soit dans le droit en vigueur, soit dans le texte adopté par le Sénat à l'alinéa 6 du présent article. L'amendement adopté par votre Commission ajoute que ces informations ne peuvent pas non plus porter sur les « *procédures et méthodes opérationnelles* » des services. En effet, elles sont le cœur du métier des services de renseignement. Il importe donc qu'elles bénéficient d'une confidentialité maximale.

Le Sénat, en adoptant un amendement de la commission des Affaires étrangères, de la défense et des forces armées, a prévu que la délégation prendrait connaissance, « *sous réserve, le cas échéant, de l'anonymisation des agents* » ⁽²⁾, des rapports de l'inspection des services de renseignement, ainsi que des rapports des services d'inspection des ministères portant sur les services de renseignement qui relèvent de leur compétence. Le Gouvernement s'est déclaré très défavorable à cette procédure au motif qu'elle méconnaîtrait le principe de séparation des pouvoirs.

L'amendement adopté par votre Commission précise que la délégation peut solliciter du Premier ministre la communication de « *tout ou partie des*

(1) Conseil constitutionnel, décision n° 2001-456 DC du 27 décembre 2001, Loi de finances pour 2002, considérant n° 42.

(2) Cette précision a été introduite par un amendement de la commission des Lois du Sénat.

rappports de l'inspection des services de renseignement », ainsi que des rapports des « *services d'inspection générale des ministères* » portant sur les services de renseignement qui relèvent de leur compétence.

En effet, votre Commission a jugé cette rédaction plus opportune que celle retenue par le Sénat à l'alinéa 6 du présent article, laquelle prévoit une transmission systématique des rapports d'inspection. Une telle transmission pourrait être interprétée comme constituant une injonction au Gouvernement, ce que la Constitution ne permet pas. De surcroît, ces inspections ont pour mission première de rendre compte au ministre concerné, voire au Premier ministre, et non au Parlement – en l'occurrence à la délégation parlementaire.

Dans cette optique, il ne semble donc pas opportun que la délégation se voie communiquer des rapports portant sur le détail de l'organisation des services. Pour autant, le contenu de certains de ces rapports pourrait lui être précieux. C'est pourquoi l'amendement adopté prévoit que le Premier ministre pourra lui transmettre tout ou partie de certains de ces rapports, dans le respect du principe de séparation des pouvoirs.

La liste des destinataires du rapport confidentiel de la délégation parlementaire au renseignement serait élargie aux ministres pour ce qui concerne les services placés sous leur autorité.

Votre Commission a adopté un amendement de votre rapporteur pour avis précisant que ces « *observations et recommandations* » adressées au président de la République et au Premier ministre le sont également au président de chaque assemblée, alors que le texte en vigueur ne prévoit qu'une simple transmission à leur attention. Il est, en effet apparu paradoxal à votre Commission que la vocation d'un organe parlementaire soit d'informer, par priorité, l'exécutif.

Votre Commission a adopté un autre amendement de votre rapporteur pour avis dont l'objectif est de regrouper au sein du **II de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958** les dispositions relatives à la composition de la délégation parlementaire au renseignement. Par ailleurs, cet amendement conduit à ce que les présidents des commissions chargées de la sécurité intérieure – les commissions des Lois – et de la défense ne soient plus membres de droit de la délégation. Ils pourront naturellement être désignés par le président de l'assemblée concernée, si ce dernier le souhaite. L'objectif poursuivi par l'amendement est d'ouvrir la délégation aux parlementaires particulièrement intéressés par cette thématique. Enfin, ces nominations se feraient – comme aujourd'hui – de manière pluraliste.

La liste des personnes pouvant être auditionnées par la délégation serait élargie au Coordonnateur national du renseignement et au directeur de l'académie du renseignement. S'agissant du Coordonnateur, il ne s'agit pas d'une innovation puisque cette précision figure déjà à l'article R*. 1122-8 du code de la défense. Sur ce point, le projet de loi ne fait qu'élever au niveau législatif une disposition réglementaire.

Par ailleurs, le Sénat a souhaité préciser qu'outre les directeurs d'administration centrale ⁽¹⁾, la délégation pourrait entendre des agents des services de renseignement « *sous réserve de l'accord et en présence du directeur du service concerné* ». Le Gouvernement s'est déclaré défavorable à cet amendement de la commission des Lois du Sénat, du fait du rejet de son sous-amendement tendant à prévoir que la délégation pouvait entendre les directeurs en fonction de ces services, « *qui peuvent se faire accompagner des collaborateurs de leur choix* ».

Votre Commission a adopté un troisième amendement de votre rapporteur pour avis dont l'objectif est de regrouper au sein du **III de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958** les prérogatives de la délégation en termes d'auditions. Il précise que les directeurs entendus peuvent « *se faire accompagner des collaborateurs de leur choix en fonction de l'ordre du jour de la délégation* ». Cette rédaction permettra à la délégation parlementaire de disposer de l'information la plus complète possible, le responsable du service demeurant son interlocuteur naturel. Alors que le texte du Sénat permet à la délégation parlementaire de choisir les agents qu'elle entend, avec l'accord préalable et en présence du directeur du service concerné, votre rapporteur pour avis propose, lui, de reprendre le texte d'un sous-amendement présenté au Sénat par le Gouvernement. En effet, l'organigramme des services étant classifié et n'entrant pas dans le champ des éléments communicables à la délégation, il ne voit pas comment celle-ci pourrait choisir seule les agents qu'elle souhaite entendre. Avec la rédaction proposée, la responsabilité du chef de service est consacrée ainsi que le pouvoir d'évocation de la délégation, par le biais de la communication de son ordre du jour.

Ce même amendement prévoit – comme le texte initial du Gouvernement – que la délégation peut inviter les présidents de la commission consultative du secret de la défense nationale et de la commission nationale de contrôle des interceptions de sécurité à lui présenter les rapports d'activité de ces commissions.

La délégation pourrait également inviter les présidents de la commission consultative du secret de la défense nationale et de la commission nationale de contrôle des interceptions de sécurité à lui présenter les rapports d'activité de ces commissions.

Le projet de loi prévoit l'absorption par la délégation parlementaire au renseignement de la commission de vérification des fonds spéciaux, qui en deviendrait une formation spécialisée (voir *infra* article 6).

(1) Sur ce point, le Sénat a supprimé toute référence à un accord préalable du ministre concerné, par un amendement de la commission des Lois ayant reçu un avis de sagesse du Gouvernement.

*

* *

La Commission est saisie de l'amendement CL2 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Le présent amendement tend à regrouper des dispositions éparpillées dans l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 décembre 1958, afin de lever toute ambiguïté dans la définition des missions de la délégation parlementaire au renseignement.

M. le président Jean-Jacques Urvoas. Cette préoccupation est louable, d'autant plus que la délégation va disposer de nouveaux pouvoirs de contrôle.

La Commission adopte l'amendement.

Elle examine ensuite l'amendement CL3 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Nous proposons que les présidents des commissions parlementaires chargées de la sécurité intérieure et de la défense ne soient plus membres de droit de la délégation parlementaire au renseignement. Cela permettra de renforcer la dimension pluraliste de celle-ci.

M. Jean-Luc Warsmann. Je partage d'autant plus votre objectif que j'étais très réservé sur cette disposition lorsqu'elle avait été votée. Cependant, il faut veiller à ce que les parlementaires nommés à la délégation ne fassent pas tous partie de la même commission. On a pu voir, durant la dernière législature, quel serait le risque : alors que la commission des Lois avait adopté à l'unanimité une modification du secret défense, ses propositions se sont heurtées à un mur ! De même, il arrive que les projets de lois relatifs aux questions militaires soient examinés devant un auditoire restreint aux commissaires de la défense, entre lesquels il n'existe pas de grandes différences d'appréciation... Une plus grande diversité serait profitable au débat et, au-delà, à l'intérêt général. Ne pourrait-on pas prévoir au moins la présence d'un membre de la commission des Lois au sein de la délégation ?

M. le rapporteur pour avis. Nous examinerons la question, mais la difficulté est de trouver la rédaction adéquate, car les parlementaires peuvent changer de commission en cours de mandat.

La Commission adopte l'amendement.

Elle en vient à l'amendement CL4 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Cet amendement tend à indiquer que la délégation parlementaire au renseignement peut entendre le Premier ministre, les

ministres compétents, le secrétaire général de la défense et de la sécurité nationale, le coordonnateur national du renseignement, le directeur de l'académie du renseignement et les directeurs en fonction des services de renseignement, et à préciser que ces derniers peuvent se faire accompagner des collaborateurs de leur choix, en fonction de l'ordre du jour de la délégation parlementaire.

M. le président Jean-Jacques Urvoas. Ce point fera probablement l'objet d'un débat en séance. Dans la mesure où les agents occupent des fonctions qui nous sont inconnues, puisque les organigrammes des services sont classifiés, il est difficile pour la délégation de demander à entendre un collaborateur précis ; inviter le directeur du service à se faire accompagner est une solution équilibrée qui devrait satisfaire tous les parlementaires qui ont travaillé sur le sujet.

La Commission adopte l'amendement.

Elle adopte l'amendement de coordination CL5 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

Puis elle en vient à l'amendement CL6 des mêmes auteurs.

M. le rapporteur pour avis. Il convient d'inverser l'ordre de transmission des observations et recommandations de la délégation parlementaire au renseignement : d'abord au Président de chaque assemblée, ensuite au président de la République et au Premier ministre.

La Commission adopte l'amendement.

Elle émet un avis favorable à l'adoption de l'article 5 modifié.

Article 6

(art. 154 de la loi n° 2001-1275 du 28 décembre 2001)

Absorption de la commission de vérification des fonds spéciaux par la délégation parlementaire au renseignement

Le présent article prévoit que la commission de vérification des fonds spéciaux deviendra une formation spécialisée de la délégation parlementaire au renseignement.

Selon l'article 154 de la loi de finances pour 2002 (n° 2001-1275 du 28 décembre 2001), la Commission est « chargée de s'assurer » que les fonds spéciaux « sont utilisés conformément à la destination qui leur a été assignée par la loi de finances ». Elle a donc pour mission d'effectuer un contrôle de régularité des comptes des dépenses réalisées sur fonds spéciaux en s'assurant de la sincérité de leur imputation comptable. Il lui appartient ainsi de vérifier que ces fonds ont bien été utilisés pour financer des dépenses qui, en raison de leur nature particulière, ne sauraient être financées par un autre truchement.

Tirant les conséquences du refus de la Cour des comptes de désigner des

représentants au sein de cette instance, la commission ne comprendrait plus, selon le présent article, de membres de la Cour des comptes, mais uniquement des parlementaires.

Le Sénat a adopté un amendement de sa commission des Affaires étrangères, de la défense et des forces armées, avec un avis favorable du Gouvernement, précisant que les deux députés et deux sénateurs siégeant à la commission de vérification sont membres de la délégation parlementaire au renseignement – cette précision figurait dans le texte initial – et sont désignés de manière à « *assurer une représentation de la majorité et de l'opposition* ».

Votre Commission a adopté un amendement de votre rapporteur pour avis précisant que le choix des membres de la commission de vérification s'effectue de manière pluraliste. En effet, si la notion d'opposition est connue ⁽¹⁾, tel n'est pas le cas de la notion de « *majorité* ».

L'amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat a supprimé la mention proposée par le Gouvernement, selon laquelle le président de la commission de vérification était choisi alternativement pour un an par le président de l'Assemblée nationale lorsque la présidence de la délégation est assurée par un sénateur et par le président du Sénat lorsque la présidence de la délégation est assurée par un député. Le Sénat a, en effet, considéré que la présidence de cette formation spécialisée qui pourrait être exercée également par le président en titre de la délégation parlementaire au renseignement.

Votre Commission a souhaité préciser que le président de la commission de vérification était choisi chaque année sans que la loi n'entre cependant dans un degré de précision trop élevé afin de consolider l'identité spécifique de la commission de vérification.

Enfin, votre Commission a adopté un autre amendement de votre rapporteur pour avis prévoyant que le rapport de la commission de vérification serait remis au Premier ministre et non pas à chacun des ministres concernés. Cette disposition est destinée à conforter la place du Premier ministre comme interlocuteur naturel des organes parlementaires chargés du contrôle du renseignement. Bien évidemment, les ministres concernés seront informés par le Premier ministre. Le dispositif adopté par votre Commission prévoit également l'information des présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances. Le président de la

(1) Cette notion figure notamment dans les articles 48 et 51-1 de la Constitution. L'article 19 du Règlement de l'Assemblée nationale prévoit, dans ses alinéas 2 et 3, la possibilité pour les groupes parlementaires de déclarer leur appartenance à l'opposition. Une telle déclaration leur ouvre plusieurs « droits spécifiques » comme l'autorise depuis la révision constitutionnelle du 23 juillet 2008 l'article 51-1 de la Constitution. En application de l'article 19, alinéa 4 du Règlement, sont par ailleurs « considérés comme groupes minoritaires ceux qui ne se sont pas déclarés d'opposition, à l'exception de celui d'entre eux qui compte l'effectif le plus élevé ». Les groupes minoritaires se voient également reconnaître des droits spécifiques en vertu du même article de la Constitution.

République et le Premier ministre – également destinataires du rapport – seraient mentionnés dans le texte après les présidents et rapporteurs généraux des commissions chargées des finances, car il pouvait paraître, de nouveau, paradoxal que la vocation d'un organe parlementaire soit d'informer, par priorité, l'exécutif.

*

* *

La Commission est saisie de l'amendement CL8 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Cet amendement vise à substituer aux mots « de la majorité et de l'opposition » le mot « pluraliste ».

La Commission adopte l'amendement.

Elle examine ensuite l'amendement CL9 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Il s'agit d'indiquer – sans entrer dans le détail – que le président de la commission de vérification est choisi chaque année.

La Commission adopte l'amendement.

Elle en vient à l'amendement CL10 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Même objet que le CL6 : il convient de modifier l'ordre de transmission des rapports.

La Commission adopte l'amendement.

Puis elle émet un avis favorable à l'adoption de l'article 6 modifié.

Article 7

(art. 656-1 du code de procédure pénale)

Audition d'agents des services de renseignement en dehors des tribunaux et des locaux des services enquêteurs

Le présent article vise à permettre, dans le cadre d'une procédure judiciaire, l'audition d'un agent d'un service de renseignement dans un lieu assurant son anonymat et la confidentialité, choisi par le chef de service, et qui peut être le lieu du service d'affectation de l'agent.

L'anonymat des agents des services de renseignement fait déjà l'objet de trois protections dans les procédures judiciaires.

— L'article 706-58 du code de procédure pénale, qui n'est pas propre aux services de renseignement, prévoit que les déclarations d'un témoin peuvent être

recueillies sans que son identité n'apparaisse dans le dossier, dans les procédures portant sur un crime ou un délit puni d'au moins trois ans d'emprisonnement et lorsque l'audition de la personne est susceptible de mettre gravement en danger sa vie ou son intégrité physique ou celles de ses proches.

— L'article 706-24 du code de procédure pénale dispose que les officiers ou agents de police judiciaire affectés dans les services de lutte contre le terrorisme peuvent être autorisés par le procureur général près la cour d'appel de Paris à déposer ou à comparaître sous un numéro d'immatriculation administrative. Ce dispositif ne peut toutefois s'appliquer aux services de renseignement que dans les limites de leurs activités de police judiciaire en matière de lutte contre le terrorisme. Il concerne donc essentiellement les officiers de police judiciaire par ailleurs agents de la direction centrale du renseignement intérieur.

— L'article 656-1 du code de procédure pénale, introduit par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), prévoit une procédure spécifique encadrant le témoignage des agents des services de renseignement appelés à comparaître. Lorsque le témoignage d'un tel agent est requis au cours d'une procédure judiciaire sur des faits dont il aurait eu connaissance lors d'une mission intéressant la défense et la sécurité nationale, son identité réelle n'apparaît pas dans la procédure. Cependant, son appartenance à un service de renseignement ou la réalité de la mission peut être attestée, en cas de contestation, par l'autorité hiérarchique de l'agent. Les auditions sont reçues dans des conditions permettant la garantie de l'anonymat de l'agent et aucune question ne peut avoir ni pour objet, ni pour effet de révéler, directement ou indirectement, son identité. Si une confrontation doit être organisée entre une personne mise en examen ou comparaisant devant la juridiction de jugement et un agent d'un service de renseignement, en raison des éléments de preuve à charge résultant de constatations personnellement effectuées par cet agent, elle doit être réalisée dans les conditions prévues par l'article 706-61 du code de procédure pénale. Dans ce cas, la voix du témoin est rendue non identifiable par des procédés techniques. Enfin, afin d'assurer le respect des droits de la défense et conformément à la jurisprudence de la Cour européenne des droits de l'homme, aucune condamnation ne peut être prononcée sur le seul fondement des déclarations recueillies selon la procédure prévue par l'article 656-1.

Selon le Gouvernement, ces trois procédures dérogatoires à la procédure pénale ordinaire n'offrent pas de garanties de protection suffisantes pour les agents des services de renseignement car la simple présence physique des agents devant une juridiction ou dans les locaux des services enquêteurs à la suite d'une convocation et leur participation à des comparutions risque, en soi, de dévoiler leur couverture et de porter atteinte à leur sécurité comme à l'efficacité de leurs missions en cours. Le Gouvernement observe, qu'en outre, tant la justice que les médias sollicitent de plus en plus fréquemment les agents des services de renseignement.

Depuis 2011, trois agents relevant du ministère de la Défense et quinze relevant du ministère de l'Intérieur ont été entendus dans le cadre de l'article 656-1 du code de procédure pénale.

Le présent article propose de modifier l'article 656-1 du code de procédure pénale pour préciser que, lorsque l'autorité hiérarchique considère que l'audition comporte des risques pour l'agent, ses proches ou son service, cette audition est faite dans un lieu assurant anonymat et confidentialité, choisi par le chef de service, et qui peut être le lieu du service d'affectation de l'agent.

*

* *

*La Commission **adopte** l'amendement de coordination CL11 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 7 **ainsi modifié**.*

Article 8

(art. L. 222-1 du code de la sécurité intérieure)

Élargissement de l'accès des services de renseignement à certains grands fichiers administratifs

Le présent article propose de modifier l'article L. 222-1 du code de la sécurité intérieure pour élargir l'accès des services de renseignement à certains fichiers administratifs.

Il concerne sept fichiers administratifs :

- le fichier national des immatriculations (FNI) ;
- le système national de gestion des permis de conduire (système d'information FAETON) ;
- le système de gestion des cartes nationales d'identité (CNI) ;
- le système de gestion des passeports (TES) ;
- le système informatisé de gestion des dossiers relatifs aux ressortissants étrangers en France (AGDREF 2) ;
- le traitement automatisé mentionné aux articles L. 611-3 à L. 611-5 du code de l'entrée et du séjour des étrangers et du droit d'asile, relatives aux ressortissants étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière, ne remplissent pas les conditions d'entrée requises (« fichier des non admis ») ;
- le système de délivrance des visas des ressortissants étrangers

(VISABIO).

La loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a prévu un accès à ces fichiers administratifs, pour les seuls services du ministère de l'Intérieur (police et gendarmerie nationales) et de la Défense et uniquement dans le cadre de la prévention et de la répression des actes terroristes.

L'article 33 de la d'orientation et de programmation pour la performance de la sécurité intérieure a élargi l'accès des services du ministère de l'Intérieur à ces fichiers à la lutte contre « *les atteintes à l'indépendance de la Nation, à l'intégrité de son territoire, à sa sécurité, à la forme républicaine de ses institutions, aux moyens de sa défense et de sa diplomatie, à la sauvegarde de sa population en France et à l'étranger et aux éléments essentiels de son potentiel scientifique et économique* ». Cette définition correspond à celle des « *atteintes aux intérêts fondamentaux de la Nation* » prévue par l'article 410-1 du code pénal.

En l'état du droit, l'accès des services de renseignement du ministère de la Défense aux fichiers reste limité à la seule lutte contre le terrorisme.

Le présent article propose de lever cette dernière restriction en permettant aux services de renseignement du ministère de la Défense, ainsi qu'à ceux relevant du ministère du Budget, d'accéder aux fichiers concernés pour les mêmes finalités que les services du ministère de l'Intérieur. Ces motifs sont, en outre, regroupés sous la définition unique de lutte contre les « *atteintes aux intérêts fondamentaux de la Nation* ».

*

* *

La Commission adopte l'amendement de coordination CL12 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

Puis elle émet un avis favorable à l'adoption de l'article 8 ainsi modifié.

Article 9

(art. L. 232-2 du code de la sécurité intérieure)

Élargissement des finalités d'accès à deux fichiers relatifs aux passagers aériens

Le présent article propose d'étendre la consultation de fichiers relatifs aux passagers aériens, par les agents des services de renseignement, à la lutte contre l'ensemble des atteintes aux intérêts fondamentaux de la Nation et non pas à la seule lutte contre le terrorisme.

L'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme a autorisé la collecte et l'exploitation des données collectées par les transporteurs aériens auprès des passagers et des agences de voyage. Ce faisant, il

a procédé à la transposition de la directive 2004/82/CE du Conseil du 29 avril 2004 relative à l'obligation pour les transporteurs de communiquer les données APIS.

Les « données passagers »

Trois catégories de données sont notamment concernées par les dispositions de l'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme

– les données « APIS » ou « API », qui comprennent le numéro et le type du document de voyage utilisé, la nationalité, le nom complet, la date de naissance, le point de passage frontalier utilisé pour entrer sur le territoire d'un État membre, le code du moyen de transport, les heures de départ et d'arrivée du transport, le nombre total de personnes transportées et le point d'embarquement initial ;

– les données « PNR » (Passenger name record), qui peuvent comprendre : les nom et prénom du passager, les renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, l'itinéraire du déplacement qui peut comporter plusieurs étapes, les indications des vols concernés (numéro des vols successifs, date, heures, classe de réservation), le nombre de personnes pour lesquelles une même réservation est faite, les coordonnées de contact du passager (numéro de téléphone au domicile, professionnel...), les tarifs accordés, l'état du paiement effectué et ses modalités, les réservations d'hôtels ou de voitures à l'arrivée, les services demandés à bord (tels que le numéro de place affecté à l'avance, les repas et les services liés à la santé, etc.) ;

– les données directement collectées à partir de la bande de lecture optique (dite « MRZ ») des documents de voyage, de la carte nationale d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires. Cette technique rend possible l'enregistrement systématique et rapide des données contenues dans la bande optique.

Le ministre de l'Intérieur est ainsi autorisé à créer des traitements automatisés des données à caractère personnel à partir d'informations recueillies à l'occasion de déplacements internationaux en provenance ou à destination d'États n'appartenant pas à l'Union européenne. Les vols intracommunautaires sont actuellement exclus du dispositif.

La loi écarte expressément l'utilisation des données dites « sensibles » au sens de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il s'agit de celles « *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ». Les données concernant les types de repas à bord ou l'état de santé du voyageur ne peuvent pas faire l'objet d'une transmission.

Les objectifs de ces traitements automatisés des données sont énumérés par l'article 7 de la loi du 23 janvier 2006 précitée. Il s'agit d'améliorer le contrôle aux frontières et la lutte contre l'immigration clandestine et de prévenir et de réprimer les actes de terrorisme.

La loi précise le champ des personnes qui peuvent accéder à ce fichier en

fonction des finalités poursuivies. S'agissant de la prévention et de la répression du terrorisme, seuls des agents individuellement désignés et dûment habilités des services spécialisés peuvent accéder à ces traitements de données. Ces traitements peuvent faire l'objet d'une interconnexion avec le fichier des personnes recherchées (FPR) et le système d'information Schengen (SIS).

Les fichiers gérés par le ministère de l'Intérieur en application de l'article 7 de la loi du 23 janvier 2006 sont :

– *le fichier national transfrontière (FNT)*, alimenté automatiquement à partir des bandes de lecture optique des documents de voyage et des données figurant sur les cartes d'embarquement et de débarquement (données APIS). En pratique, ce système ne concerne que les passagers aériens en provenance ou à destination de cinq pays (Afghanistan, Iran, Pakistan, Syrie et Yémen).

– *le fichier des passagers aériens (FPA) et le système européen de traitement des données d'enregistrement et de réservation (SETRADER)*. Le premier de ces deux fichiers reposait sur une expérimentation de collecte de données APIS pour les seuls vols en provenance ou à destination de certains États, qui s'est achevée le 31 décembre 2011. Actuellement, c'est le fichier SETRADER qui est actif. Sa création a été autorisée par un arrêté interministériel du 11 avril 2013.

La consultation par les services de renseignement de ces fichiers est actuellement limitée à la seule lutte contre le terrorisme. Le présent article propose d'étendre cette consultation à la lutte contre l'ensemble des atteintes aux intérêts fondamentaux de la Nation.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 9 sans modification.

Article 10

(art. L. 232-7 [nouveau] du code de la sécurité intérieure)

Création à titre expérimental d'un nouveau traitement relatif aux données des transporteurs aériens

Le présent article permet de créer un nouveau fichier de données PNR (« *Passenger name record* »), anticipant ainsi le vote d'une directive européenne dont le projet a été présenté en février 2011. Ce fichier serait placé sous la responsabilité des ministres chargés de l'intérieur, de la défense, des transports et des douanes. Il serait mis en œuvre, comme le prévoirait la directive, par une « unité de renseignement passagers » ou « unité d'information passagers » (UIP) composée de membres des services de la douane, de la police et de la gendarmerie.

Ce fichier, qui sera utilisé par les services de police, de gendarmerie et par les services de renseignement, aurait pour finalité de contribuer tant à la prévention qu'à la répression judiciaire de certaines infractions considérées comme particulièrement graves (criminalité organisée, terrorisme, atteintes aux intérêts fondamentaux de la Nation).

Le présent article propose d'introduire un nouvel article L. 232-7 dans le code de la sécurité intérieure afin de prévoir la mise en œuvre de ce traitement de données à caractère personnel.

Il concernerait l'ensemble des vols à destination et en provenance du territoire national, à l'exception des vols reliant deux points de la France métropolitaine.

Les modalités d'application seront fixées par un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Ce décret déterminera les services ayant accès aux données en précisant si cet accès est autorisé à des fins de répression ou à des fins de prévention. Enfin, ce nouveau système automatisé de traitement des données serait créé à titre temporaire, puisqu'il ne s'appliquerait que jusqu'au 31 décembre 2017.

La commission des Affaires étrangères, de la défense et des forces armées du Sénat a souhaité préciser que les données collectées ne pourront être conservées que cinq ans.

En séance publique, le Sénat a adopté un amendement de sa commission des Lois, avec l'accord du Gouvernement, afin de préciser que les services autorisés à accéder à ces données pourront « *interroger l'unité de gestion chargée de la collecte des données auprès des transporteurs aériens* » et que ce décret prévoira les conditions de leur conservation et de leur analyse.

En effet, le projet de directive prévoit que les données transmises par les passagers aériens ne seront pas *directement* transférées aux services répressifs ou de renseignement qui les utiliseront pour mener leurs investigations, mais d'abord traitées par une unité de gestion, chargée de gérer le traitement automatisé, de s'assurer de l'exactitude des données, d'évaluer le risque présenté par les passagers pour décider ou non d'alerter les services compétents.

Votre Commission a adopté un amendement de votre rapporteur pour avis visant à garantir pleinement la confidentialité des informations personnelles sensibles.

Seraient ainsi exclues de ce traitement automatisé les données à caractère personnel susceptibles de révéler l'origine ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, ou les données qui concernent la santé ou la vie sexuelle de l'intéressé.

Ce faisant, l'amendement de votre Commission réaffirme la primauté de la garantie des libertés publiques fondamentales dans le cadre de ce traitement automatisé de données à caractère personnel.

*

* *

La Commission est saisie de l'amendement CL13 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Cet amendement vise à garantir la confidentialité des informations personnelles sensibles.

La Commission adopte l'amendement.

Puis elle émet un avis favorable à l'adoption de l'article 10 ainsi modifié.

Article 11

(art. L. 234-2 du code de la sécurité intérieure)

Accès des services du ministère de la défense aux fichiers de police judiciaire dans le cadre des enquêtes administratives

Le présent article vise à rendre possible une consultation directe des fichiers d'antécédents judiciaires par des agents individuellement désignés et spécialement habilités des services spécialisés de renseignement désignés par le ministère de la Défense.

L'article 230-6 du code de procédure pénale permet aux services de police et de gendarmerie de mettre en œuvre des traitements automatisés de données à caractère personnel visant à faciliter la constatation des infractions. Cet article constitue la base juridique du système de traitement des infractions constatées (STIC), du fichier JUDEX ainsi que du traitement d'antécédents judiciaires (TAJ) qui doit remplacer ces deux fichiers.

La loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure a permis la consultation de ces fichiers pour la réalisation d'enquêtes administratives, prévues par l'article 114-1 du code de la sécurité intérieure. Il s'agit de vérifier, préalablement à un recrutement, une affectation, un agrément ou une autorisation, que la personne concernée a eu un comportement compatible avec l'exercice des fonctions envisagées.

Cependant, en l'état du droit, l'article L. 234-2 du code de la sécurité intérieure limite aux seuls policiers et gendarmes l'accès aux fichiers d'antécédents judiciaires dans le cadre d'une enquête administrative. Les services de renseignement du ministère de la Défense doivent donc s'adresser aux services de police ou de gendarmerie pour obtenir les renseignements nécessaires.

Les agents des services de renseignement du ministère de la défense peuvent pourtant avoir besoin de s'assurer de l'honorabilité de personnes susceptible d'exercer des fonctions sensibles ou accéder à des informations protégées par le secret de la défense nationale. C'est l'objet du présent article.

*

* *

*La Commission **adopte** l'amendement de coordination CL14 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 11 **ainsi modifié**.*

Article 12

(art. L. 234-3 du code de la sécurité intérieure)

Accès des services du ministère de la Défense aux fichiers de police judiciaire dans le cadre des enquêtes administratives pour l'exercice de missions ou d'interventions

Le présent article tend à permettre aux agents des services de renseignement du ministère de la Défense d'accéder aux fichiers d'antécédents judiciaires dans le cadre des enquêtes administratives pour l'exercice de leur mission de protection des personnels du ministère.

L'article L. 234-3 du code de la sécurité intérieure, issu de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, prévoit que les agents de la police et de la gendarmerie nationales peuvent accéder aux fichiers d'antécédents judiciaires pour l'« *exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense visés à l'article 17 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense* ».

Le présent article ouvre cette possibilité de consultation aux agents des services de renseignement du ministère de la Défense, « *dans la limite de leurs attributions* » et « *aux fins de protection de la sécurité de leurs personnels* » et dans des conditions fixées par décret en Conseil d'État.

*

* *

*La Commission émet un avis **favorable** à l'adoption de l'article 12 **sans modification**.*

Article 13

(art. L. 34-1 et L. 34-1-1 du code des postes et des communications électroniques, art. 6 de la loi n° 2004-575 du 21 juin 2004 et art. L. 222-2, L. 222-3, L. 243-7, L. 245-3, L. 243-12, L. 246-1 à L. 246-5 [nouveaux] du code de sécurité intérieure)

Clarification du cadre juridique relatif à la géolocalisation en temps réel

Le présent article vise à clarifier le cadre juridique relatif à la géolocalisation en temps réel. Sa rédaction résulte de l'adoption par le Sénat, avec l'avis favorable du Gouvernement, d'un amendement de sa commission des Lois.

Les services de renseignement peuvent obtenir communication des données techniques de connexion des personnes qu'ils surveillent – les fameuses « fadettes » – qui peuvent contenir des données de localisation.

En effet, la loi n° 2006-64 du 23 janvier 2006 a introduit, au sein du code des postes et des communications électroniques, un article L. 34-1-1 qui permet aux personnes habilitées d'exiger des opérateurs de communications électroniques la transmission de « *données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* »⁽¹⁾.

En d'autres termes, cette disposition permet, *mais uniquement dans le cadre de la lutte anti-terroriste*, d'avoir connaissance des données figurant sur les factures détaillées (identité des personnes entrées en communication, date et durée de l'échange), de localiser un téléphone portable ou un ordinateur, mais aussi de connaître les données de connexion Internet (numéro de protocole, date et durée des connexions). Ce dispositif, initialement prévu à titre provisoire⁽²⁾, a été prolongé jusqu'au 31 décembre 2015 par la loi du 21 décembre 2012⁽³⁾.

Ce dispositif fonctionne sur la base d'une saisine obligatoire d'une personnalité qualifiée placée auprès du ministre de l'Intérieur, d'une mise en œuvre par la plate-forme de l'unité de coordination de la lutte anti-terroriste (UCLAT) et d'un contrôle *a posteriori* par la commission nationale des interceptions de sécurité (CNCIS).

Les données de connexion sont notamment utilisées par les services spécialisés à des fins de géolocalisation d'objets tels que des téléphones mobiles.

(1) Article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

(2) L'article 32 de la loi du 23 janvier 2006 précitée prévoyait initialement que ces dispositions n'étaient applicables que jusqu'au 31 décembre 2008. La loi n° 2008-1245 du 1^{er} décembre 2008 visant à prolonger l'application des articles 3, 6 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a prorogé de quatre ans cette application, soit jusqu'au 31 décembre 2012.

(3) Loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme.

Ceci permet de suivre les déplacements de ces objets, et par conséquent des personnes qui les détiennent, à intervalles réguliers ou en temps réel. Or, la rédaction actuelle du premier alinéa de l'article L. 34-1-1 laisse penser que les demandes ne peuvent porter que sur des données de connexion « *conservées* », donc après l'utilisation d'un téléphone portable, rendant impossible le suivi en temps réel d'une « *cible* » des services.

En conséquence, le présent article, dans sa version initiale, proposait d'autoriser les services spécialisés à exiger des opérateurs les données « *traitées par les réseaux ou les services de communication électroniques de ces derniers, après conservation* ou en temps réel, *impliquant le cas échéant une mise à jour de ces derniers* ».

La Cour européenne des droits de l'homme, dans un arrêt du 2 septembre 2010 ⁽¹⁾ a estimé qu'un dispositif de géolocalisation pouvait être acceptable au regard du droit au respect de la vie privée garanti par le paragraphe 1 de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, à condition que la loi soit très précise dans sa description du dispositif.

Le dispositif de droit commun s'agissant des interceptions de sécurité administratives n'est pas celui de l'article L. 34-1 du code des postes et télécommunications, qui ne traite que des « données de connexions », inséré par la loi du 23 janvier 2006 et visé par le présent article, mais celui des articles L. 241-1 et suivants du code de la sécurité intérieure, issu de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, qui traite, de manière générale, des interceptions de sécurité.

La commission des Lois du Sénat a estimé que la géolocalisation en temps réel d'une personne semblait plus proche, en termes d'atteinte aux libertés, de l'interception d'une communication que du simple recueil de données de connexion. Elle a également observé que le fait que la géolocalisation soit insérée dans l'article L. 34-1-1 du code des postes la cantonnait à un usage anti-terroriste, alors même que les services de renseignement pourraient en avoir besoin pour les finalités beaucoup plus larges prévues par le dispositif issu de la loi du 10 juillet 1991. Elle a donc souhaité opérer la fusion des deux dispositifs annoncée en décembre 2012 par le ministre de l'Intérieur à l'occasion de l'examen parlementaire de la loi du 21 décembre 2012 précitée.

Le Sénat a ainsi adopté un amendement de sa commission des Lois insérant, au sein du code de la sécurité intérieure, un dispositif complet de recueil administratif des données techniques de connexion et de géolocalisation en temps réel, applicable au 1^{er} janvier 2015.

Le texte adopté par le Sénat regroupe, au sein d'un nouveau chapitre VI du titre IV du livre II du code de la sécurité intérieure des dispositions relatives à

(1) CEDH, 2 septembre 2010, Uzun c/. Allemagne.

l'accès administratif aux données de connexion, qui se trouveront donc dans le même titre que celles relatives aux interceptions de sécurité. Ce nouveau chapitre, prévu par le 2° du I du présent article, contiendrait cinq articles : L 246-1 à L. 246-5.

Par coordination, le 1° du I du présent article modifie l'intitulé du titre IV du livre II du code de la sécurité intérieure pour y ajouter l'« accès administratif aux données de connexion » aux « interceptions de sécurité ».

Le nouvel article L. 246-1 précise que, pour les finalités énumérées à l'article L. 241-2⁽¹⁾, peut être autorisé le recueil, auprès des opérateurs de communications électroniques, des « informations ou documents traités ou conservés » qu'ils détiennent, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électronique, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Ce faisant, ce dispositif propose un dispositif unique de recueil administratif des données de connexion, qu'il s'agisse de données relatives aux communications passées (les factures détaillées ou « fadettes ») ou à la localisation des équipements permettant ces communications.

Le présent article étend donc les capacités d'accéder à ces données à l'ensemble des services de renseignement – et non aux seuls services relevant du ministère de l'Intérieur – et pour tous les motifs liés à la défense des intérêts fondamentaux de la Nation. Sur le fond, il s'agit plutôt d'une simplification de notre droit car ces services pouvaient déjà accéder aux données techniques de connexion du fait de la jurisprudence de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) datant de 2010. Depuis lors, elle estime que les facturations détaillées et les identifications relèvent de la phase préparatoire à l'interception telle qu'elle est prévue par l'article L. 244-2 du code de la sécurité intérieure.

Deux régimes cohabitent donc aujourd'hui :

— **en matière de prévention du terrorisme**, seuls les services du ministère de l'Intérieur, selon l'article L. 34-1-1 du code des postes et des communications électroniques, issu de la loi du 23 janvier 2006⁽²⁾, peuvent exiger

(1) Il s'agit de la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous.

(2) Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

des opérateurs les « fadettes »⁽¹⁾.

— **dans les autres domaines liés à la protection des intérêts fondamentaux de la Nation**, les dispositions de l'article L. 244-2 du code de la sécurité intérieure permettent aux services du ministère de l'Intérieur ainsi qu'à l'ensemble des services de renseignement, de solliciter ces données auprès des opérateurs téléphoniques et des fournisseurs d'accès à internet.

Le nouvel article L. 246-2 prévoit, dans son I, que ces « *informations ou documents* » sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2. Corrélativement, le présent article (dans le **3° du I**) abroge, par voie de conséquence, les articles L. 222-2 et L. 222-3 du code de la sécurité intérieure qui permettent aux policiers et gendarmes chargés de la lutte anti-terroriste d'accéder aux données conservées par les opérateurs de communications électroniques (article L. 222-2) ou aux données conservées par les prestataires de services de communication au public en ligne (article L. 222-3).

Ce même article L. 246-2, dans son II, précise que les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre, désignée pour une durée de trois ans renouvelable par la CNCIS sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms.

Le présent article reprend intégralement le dispositif actuellement applicable pour les « fadettes », tel que prévu au quatrième alinéa de l'article L. 34-1-1 du code des postes et des communications électroniques.

Le nouvel article L. 246-3 prévoit la possibilité de transmission *en temps réel* des données de connexions et, donc, de localisation.

Ce nouveau dispositif serait mis en œuvre sur autorisation du Premier ministre, sur la base d'une demande écrite et motivée des ministres en charge de la sécurité intérieure, de la défense, de l'économie et du budget (ou des personnes que chacun d'eux aura spécialement désignées), pour une durée maximale de dix jours. Elle peut être renouvelée dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la CNCIS.

Votre Commission a adopté un amendement de votre rapporteur pour avis visant à aligner la durée d'une autorisation émise au titre du présent article pour la

(1) *L'article prévoit la transmission de « données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».*

géolocalisation sur celle applicable en matière d'interception de sécurité, soit quatre mois. En effet, le procédé de géolocalisation s'avérant moins intrusif dans la vie privée qu'une interception de sécurité, il serait curieux que la durée d'utilisation soit plus courte pour ce mode d'intervention.

La procédure proposée par le présent article est en tout point comparable à celle applicable, selon l'article L. 243-8 du code de la sécurité intérieure, aux interceptions de sécurité. En effet, si le président de la CNCIS estime que la légalité de la décision du Premier ministre au regard des motifs prévus à l'article L. 241-2 du même code n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication. Dans le cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions les encadrant, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

Le nouvel article L. 246-4 prévoit que la CNCIS dispose d'un accès permanent au dispositif de recueil de données techniques mis en œuvre en application du chapitre VI du titre IV du livre II du code de la sécurité intérieure afin de procéder à des contrôles visant à s'assurer du respect des conditions légales.

Ce dispositif reprend celui prévu à l'article L. 243-12 du même code, qui déterminera la compétence de la CNCIS pour le contrôle des accès aux données de connexion. Il prévoit, en outre, d'étendre cette compétence à la nouvelle possibilité de transmission *en temps réel* des données de connexions. C'est donc logiquement que le présent article (**dans le 3° du I**) abroge l'article L. 243-12 précité.

Le nouvel article L. 246-5 prévoit que les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs pour répondre aux demandes de données de connexion font l'objet d'une compensation financière. Cette disposition est actuellement prévue par le troisième alinéa de l'article L. 34-1-1 du code des postes et des communications électroniques.

Le **4° du I** du présent article procède à une coordination au sein de l'article L. 243-7 du code de la sécurité intérieure, relatif au rapport public de la CNCIS.

Le **5° du I** du présent article procède à une coordination au sein de l'article L. 245-3 du même code, relatif aux sanctions applicables aux opérateurs qui refuseraient de permettre l'accès aux données de connexion.

Le **II** du présent article prévoit l'abrogation de l'article L. 34-1-1 du code des postes et des communications électroniques, dont les dispositions sont reprises dans le code de la sécurité intérieure.

Le **III** du présent article prévoit l'abrogation du *II bis* de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,

dont les dispositions relatives à l'accès aux données de connexion dans le cadre de la prévention du terrorisme, sont reprises dans le code de la sécurité intérieure.

Enfin, le **IV** du présent article prévoit que l'ensemble de ses dispositions entrera en vigueur le 1^{er} janvier 2015.

*

* *

La Commission est saisie de l'amendement CLI5 du rapporteur pour avis et de M. le président Jean-Jacques Urvoas.

M. le rapporteur pour avis. Cet amendement tend à porter la durée des autorisations de géolocalisation à quatre mois.

M. le président Jean-Jacques Urvoas. Notons que, sur le même thème, nous aurons à traiter assez rapidement d'une autre question, puisque la Cour de cassation vient de décider que le recours à la géolocalisation dans le cadre d'une enquête préliminaire était sans fondement lorsqu'elle était demandée par un procureur, au motif que celui-ci ne peut pas être assimilé à un magistrat indépendant – en tout cas, pas selon la jurisprudence de la Cour européenne des droits de l'homme (CEDH). Cette décision, qui a été relayée très rapidement par la Chancellerie, va entraîner l'interruption de plusieurs enquêtes préliminaires et certains suspects vont se retrouver sans surveillance de la part des services de police judiciaire. Le Gouvernement et les professionnels travaillent à pallier cette carence, et je ne doute pas que la Commission sera bientôt saisie d'une proposition en ce sens.

La Commission adopte l'amendement.

Puis elle émet un avis favorable à l'adoption de l'article 13 ainsi modifié.

CHAPITRE III

Dispositions relatives à la protection des infrastructures vitales contre la cybermenace

Article 14

(art. L. 2321-1 et L. 2321-2 [nouveaux] du code de la défense)

Renforcement du dispositif étatique en matière de cyberdéfense

Le présent article a deux objets. Il vise tout d'abord à consacrer la compétence du Premier ministre en matière de protection et de défense des systèmes d'information. Il a également pour objet de reconnaître aux services concernés de l'État la possibilité de prendre une série de mesures de lutte informatique défensive en cas d'attaque informatique.

En premier lieu, le présent article propose, dans un nouvel article

L. 2321-1 dans le code de la défense, de consacrer explicitement la responsabilité du Premier ministre en matière de définition de la politique et de la coordination de l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Ce faisant, il consacre également la fonction d'autorité nationale de défense des systèmes d'information, qui est confiée à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), service du Premier ministre rattaché au Secrétaire général de la défense et de la sécurité nationale.

En second lieu, le présent article prévoit, dans un nouvel article L. 2321-2 dans le code de la défense, de permettre à l'État de prendre des mesures de lutte informatique défensive en cas d'attaque informatique portant atteinte au potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la Nation. En effet, de telles actions risqueraient, sans cette base légale, d'enfreindre deux dispositions du code pénal.

L'article 323-3-1 du code pénal prohibe la détention, sans motif légitime, de programmes informatiques susceptibles de porter atteinte aux systèmes de traitement automatisé de données. Pourtant, les services de l'État ont besoin de les analyser pour comprendre le fonctionnement des attaques.

De même, l'article 323-1 du code pénal réprime les accès frauduleux aux systèmes de traitement automatisé de données. Or, les services de l'État peuvent avoir besoin d'accéder aux systèmes à l'origine de l'attaque pour rechercher des données permettant de comprendre le fonctionnement de l'attaque informatique.

Le présent article prévoit donc explicitement ces différentes actions pouvant être effectuées par les services de l'État. Ainsi autorisées, celles-ci ne sont ainsi plus susceptibles d'être des infractions au sens des articles 323-1 et 323-3-1 du code pénal.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 14 sans modification.

Article 15

(art. L. 1332-6-1 à L. 1332-6-6 [nouveaux] et L. 1332-7 du code de la défense)

Renforcement des obligations des opérateurs d'importance vitale en matière de sécurité et de défense des systèmes d'information

Le présent article propose de renforcer les obligations des opérateurs d'importance vitale en matière de sécurité et de défense des systèmes d'information.

Les opérateurs d'importance vitale – environ 250⁽¹⁾ – sont ceux « dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation », selon l'article L. 1332-1 du code de la défense.

Le présent article propose de créer une nouvelle section 2, intitulée « Dispositions spécifiques à la sécurité des systèmes d'information », au chapitre II du titre III de la première partie de la partie législative du code de la défense, qui comprendrait six nouveaux articles L. 1332-1 à L. 1332-6, ainsi que l'article L. 1332-7, qui serait modifié.

Le nouvel article L. 1332-6-1 du code de la défense prévoit que le Premier ministre peut imposer des règles aux opérateurs d'importance vitale concernant la protection de leurs systèmes d'information critiques. Il est précisé que les opérateurs seront tenus d'appliquer ces règles à leurs frais.

Le nouvel article L. 1332-6-2 du même code prévoit que les opérateurs d'importance vitale ont une obligation de notification systématique et sans délai des incidents informatiques au Premier ministre.

Le nouvel article L. 1332-6-3 du même code est d'étendre la capacité de contrôle et d'audit de l'État à l'ensemble des secteurs d'activité d'importance vitale. En effet, l'article L. 33-10 du code des postes et des communications électroniques limite cette possibilité pour l'État à la seule sécurité des réseaux des opérateurs de communications électroniques.

Le nouvel article L. 1332-6-4 du même code donne la possibilité au Premier ministre d'imposer, en cas de crise informatique majeure, les mesures techniques nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale.

Le nouvel article L. 1332-6-5 du même code oblige l'État à préserver la confidentialité sur les informations recueillies auprès des opérateurs d'importance vitale.

Le présent article prévoit, en outre, de modifier l'article L. 1332-7 du code de la défense afin de préciser les sanctions pénales encourues par les opérateurs d'importance vitale en cas de non-respect des obligations prévues précédemment. Ces sanctions sont alignées sur celles prévues par ce même article pour la protection physique des installations d'importance vitale. Le non-respect de l'une de ces obligations sera passible d'une amende de 150 000 euros pour les personnes physiques et d'une amende de 750 000 euros pour les personnes morales.

(1) La liste des opérateurs d'importance vitale est classifiée.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 15 sans modification.

Article 16

(art. 226-3 et 226-15 du code pénal)

Extension de la liste des équipements informatiques soumis au régime d'autorisation

Le présent article propose d'étendre la liste des équipements informatiques soumis au régime d'autorisation.

En l'état du droit, l'article 226-3 du code pénal soumet à autorisation les appareils conçus pour porter atteinte au secret des correspondances, atteinte qui constitue l'infraction prévue à l'article 226-15 du code pénal. Les catégories d'appareils relevant de cette procédure sont définies par l'arrêté du Premier ministre du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal.

Les évolutions technologiques ont pour effet que de plus en plus d'équipements de réseau, sans être des moyens d'interception, possèdent des fonctions qui pourraient être utilisées pour intercepter le trafic du réseau. N'étant pas conçus pour les interceptions, ces équipements ne sont actuellement pas soumis à l'autorisation prévue par l'article 223-3 du code pénal, qui ne porte que sur les appareils « *conçus pour réaliser* » les interceptions.

Le présent article a donc pour objet d'étendre le contrôle de l'État aux équipements qui, sans être conçus pour permettre les interceptions de communication de données informatiques ou de correspondances, sont susceptibles d'être utilisés à ces fins. Il est donc proposé de remplacer à l'article 226-3 du code pénal les mots « *conçus pour réaliser les opérations* » par les mots « *susceptibles de permettre la réalisation d'opérations* » et de procéder à une coordination à l'article 226-15 du même code.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 16 sans modification.

Article 16 bis

(art. L. 2321-3 [nouveau] du code de la défense et L. 336-3 et L. 34-1 du code des postes et des communications électroniques)

Accès aux coordonnées des utilisateurs des adresses Internet pour les besoins de la sécurité informatique

Le présent article, introduit par un amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, vise à reconnaître la possibilité, pour les agents habilités et assermentés de l'agence nationale de sécurité des systèmes d'information (ANSSI), d'obtenir des opérateurs de communications électroniques l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information afin de les alerter sur la vulnérabilité ou la compromission de leur système.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 16 bis sans modification.

Article 16 ter

(art. 323-3-1 du code pénal et L. 122-6-1 du code de la propriété intellectuelle)

Possibilité d'exercer une activité de recherche ou de développement de produits ou de service de sécurité informatique

Le présent article, introduit par un amendement de la commission des Affaires étrangères, de la défense et des forces armées du Sénat, vise à clarifier et à renforcer la sécurité juridique de l'activité de recherche en matière informatique, afin de développer des produits ou services de sécurité.

Dans le droit en vigueur, l'article 323-3-1 du code pénal interdit, sauf motif légitime, l'importation, la détention, l'offre, la cession ou la mise à disposition de programmes exploitant les failles ou les vulnérabilités de logiciels. Il convient cependant de permettre, à des fins de recherche et de développement, de mettre en œuvre de tels programmes, de manière encadrée.

Le présent article propose donc de clarifier la rédaction de l'article 323-3-1 du code pénal. Il a également pour objet de modifier la rédaction de l'article L. 122-6-1 du code de la propriété intellectuelle afin de préciser qu'il est possible, sans l'autorisation de l'auteur, observer, étudier ou tester non seulement le fonctionnement d'un logiciel mais aussi sa sécurité.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 16 ter sans modification.

CHAPITRE IV

Dispositions relatives au traitement pénal des affaires militaires

Article 17

(art. L. 211-7 du code de justice militaire)

Régime de présomption en cas de mort violente d'un militaire lors d'une action de combat, à l'occasion d'une opération militaire à l'étranger

Le présent article instaure une présomption simple, selon laquelle la mort violente d'un militaire, au cours d'une action de combat lors d'une opération militaire, est présumée ne pas avoir une cause inconnue ou suspecte.

Aujourd'hui, les dispositions de droit commun de l'article 74 du code de procédure pénale s'appliquent en cas de mort violente d'un militaire lors d'une opération militaire à l'étranger. Cet article permet de déclencher une enquête pour recherche des causes de la mort, lorsqu'un cadavre ou qu'une personne grièvement blessée est découvert et que les causes de cette mort ou de ces blessures sont inconnues ou suspectes.

L'enquête en recherche des causes de la mort n'a pas vocation à se substituer à l'enquête pénale proprement dite. Si les circonstances de la mort sont éclaircies, cette enquête s'achève et conduit soit à un classement sans suite, si les causes de la mort ne sont pas délictuelles ou criminelles, soit à l'ouverture d'une enquête, dans le cas contraire.

Le code de justice militaire distingue le temps de guerre et le temps de paix et prévoit des règles distinctes. Pour autant, l'ensemble des opérations extérieures se déroule, formellement, en temps de paix. L'article L. 211-7 du code de justice militaire prévoit qu'en temps de paix, en cas de découverte d'un cadavre, les officiers de police judiciaire des forces armées et le procureur de la République du tribunal de grande instance de Paris « appliquent les règles de l'article 74 du code de procédure pénale ».

Le présent article instaure une présomption simple selon laquelle la mort d'un militaire au cours d'une action de combat, dans le cadre d'une opération militaire à l'extérieur du territoire français n'est ni de cause inconnue, ni de cause suspecte. Il propose donc de réécrire l'article L. 211-7 du code de justice militaire pour préciser que la mort violente d'un militaire lors « *d'une action de combat se déroulant dans le cadre d'une opération militaire hors du territoire de la République* » est présumée ne pas avoir de cause suspecte ou inconnue.

S'agissant d'une présomption simple, l'officier de police judiciaire des forces armées ne pourra ouvrir d'enquête sur les recherches de cause de la mort que s'il apporte des éléments selon lesquels les circonstances de la mort sont inconnues ou suspectes.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 17 sans modification.

Article 18

(art. 698-2 du code de procédure pénale et L. 211-7 du code de justice militaire)

Mise en mouvement de l'action publique à l'encontre de militaires engagés dans une opération militaire en dehors du territoire français

Le présent article propose de confier au ministère public le monopole de la mise en mouvement de l'action publique, pour tout fait commis par un militaire dans le cadre de sa mission, lors d'une « *opération militaire se déroulant hors du territoire français* ». Cette notion d'opération a été précisée par le Sénat.

La mise en mouvement de l'action publique à l'encontre de tout Français à l'étranger est réservée au seul ministère public, *en matière de délits*. C'est l'application de l'article 113-8 du code pénal. *En matière de crimes*, le régime est celui qui est applicable sur le territoire français : les victimes peuvent se constituer partie civile devant un juge d'instruction pour surmonter un refus de poursuivre du parquet.

Pourtant, l'article L. 211-11 du code de justice militaire prévoit un régime dérogatoire pour les militaires à l'étranger : *en matière de délit*, le ministère public n'a pas le monopole des poursuites quand est en cause un militaire en mission à l'étranger. Les victimes peuvent donc se constituer partie civile.

Le présent article propose de modifier l'article L. 211-11 du code de justice militaire pour introduire une référence à l'article 113-8 du code pénal : le ministère public aura désormais le monopole des poursuites contre un Français, à l'étranger, que celui-ci soit militaire en mission ou non.

Par ailleurs, il modifie l'article 698-2 du code de procédure pénale pour prévoir que l'action publique portant sur « *des faits commis dans l'accomplissement de sa mission par un militaire engagé dans le cadre d'une opération militaire se déroulant hors du territoire français* » ne peut être mise en mouvement que par le parquet, qu'il s'agisse de délits *ou de crimes*.

La commission des Affaires étrangères, de la défense et des forces armées du Sénat a adopté un amendement substituant aux termes généraux d'« *opération militaire* » l'expression « *opération mobilisant des capacités militaires* », qui permet en effet de prendre en compte la variété des opérations menées par les armées.

Le présent article procède ainsi à un alignement, *en matière de délits*, sur le droit commun actuellement applicable pour tous les ressortissants français à

l'étranger. Il crée, en revanche une dérogation à ce même droit commun en ce qui concerne *les crimes* éventuellement commis dans l'accomplissement de leur mission par les militaires. Selon le ministère de la Défense, le monopole des poursuites du parquet en la matière se justifie par le caractère particulier des missions exécutées par les militaires.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 18 sans modification.

Article 19

(art. L. 4123-11 et L. 4123-12 du code de la défense)

Responsabilité pénale des militaires

Le présent article modifie les articles L. 4123-11 et L. 4123-12 du code de la défense qui définissent un régime particulier de mise en cause de la responsabilité pénale des militaires, lorsqu'ils exercent leurs missions, en prenant en compte, d'une part, les spécificités de l'action de combat, pour éviter une mise en cause en application du régime de droit commun, en cas de commission d'une infraction non intentionnelle et, d'autre part, en précisant les conditions d'application de l'excuse pénale permettant aux militaires d'utiliser la force en dehors des cas de légitime défense.

Le présent article précise les éléments au regard desquels la « *diligence normale* » doit être appréciée. Il établit ainsi une liste, non limitative, d'éléments au regard desquels ces diligences normales sont appréhendées : l'urgence dans laquelle la mission est exercée, les informations dont les militaires ont disposé au moment de l'action, et les circonstances liées à l'action de combat.

L'article L. 4123-12 du code de la défense prévoit une excuse pénale propre aux seuls militaires. Il leur autorise l'usage de la force en dehors des cas de légitime défense, dans deux cas : lorsqu'ils participent à une opération militaire à l'extérieur du territoire, dans le respect du droit international et si cela est « *nécessaire à l'accomplissement de la mission* » et dans le cas spécifique de la défense d'une « *zone hautement sensible* » définie comme « *la zone définie par voie réglementaire à l'intérieur de laquelle sont implantés ou stationnés des biens militaires dont la perte ou la destruction serait susceptible de causer de très graves dommages à la population, ou mettrait en cause les intérêts vitaux de la défense nationale* »,

Le présent article précise, dans ce contexte, au II de l'article L. 4123-12 du code de la défense, la notion d'opération militaire pour englober toutes les opérations militaires sans opérer de distinction en fonction de leur objet, de leur durée ou de leur ampleur, afin de ne pas exclure du champ de ce dispositif des

opérations très ponctuelles et de prendre en compte la diversité croissante de ces opérations militaires : libération d'otages, lutte contre la piraterie ou évacuation de ressortissants. La commission des Affaires étrangères, de la défense et des forces armées du Sénat a, comme à l'article 18, préféré retenir la notion d'« *opération mobilisant des capacités militaires* ».

*

* *

La Commission émet un avis favorable à l'adoption de l'article 19 sans modification.

Article 20

(art. L. 211-5 et L. 211-22 du code de justice militaire
et art. 698-5 du code de procédure pénale)

Correction d'erreurs formelles résultant de la suppression du Tribunal aux armées de Paris et précision sur la procédure applicable aux militaires en temps de paix

Le présent article procède à diverses coordinations formelles. Il s'agit, notamment, de remplacer des mentions du « *Tribunal aux Armées de Paris* » par des références aux « *juridictions spécialisées en matière militaire* » et à modifier des mentions relatives aux « *juridictions des forces armées* » (art. 211-5 du code de justice militaire), ou au « *tribunal aux armées* » (art. 211-22 du code de justice militaire). En effet, depuis la loi n° 2011-1863 du 13 décembre 2011 relative à la répartition des contentieux et à l'allègement de certaines procédures juridictionnelles, les « *juridictions des forces armées* » n'existent plus en temps de paix. Cette dernière notion doit donc être remplacée par celle de « *juridictions spécialisées en matière militaire* ».

Par ailleurs, le présent article insère, dans l'article 698-5 du code de procédure pénale qui liste les articles du code de justice militaire applicable à un militaire en temps de paix, une référence à l'article L. 211-24 du code de justice militaire. Ce dernier article, rendu donc applicable aux militaires, prévoit qu'après un non-lieu, en cas de réouverture d'une information au regard de charges nouvelles, l'avis du ministre ou des personnes qu'il a désigné doit être recueilli au préalable par le procureur de la République, qui n'est pas lié par et avis.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 20 sans modification.

Article 21

(art. 697 du code de procédure pénale)

Spécialisation des juridictions en matière militaire

Le présent article vise à rationaliser la carte judiciaire des juridictions de droit commun spécialisées en matière militaire.

Il existe actuellement une juridiction spécialisée en matière militaire par ressort de cour d'appel et leur charge de travail est très variable.

Le présent article propose de regrouper ces juridictions au sein de pôles interrégionaux. Cette rationalisation permettra une meilleure spécialisation des juridictions, implantées désormais sur le ressort de plusieurs cours d'appel. Ce redécoupage sera effectué par un décret commun du ministre de la Justice et du ministre de la Défense.

*

* *

La Commission émet un avis favorable à l'adoption de l'article 21 sans modification.

CHAPITRE V

Dispositions relatives aux ressources humaines

Section 1

Dispositions relatives à la protection juridique

Article 22

Extension de la protection fonctionnelle aux ayants-droit des militaires décédés en opérations et à certains personnels civils

Le présent article a pour objet d'étendre aux ayants droit des militaires décédés à raison de leurs fonctions la protection fonctionnelle. Il crée également un dispositif spécifique pour les ayants droit de certains agents civils du ministère de la Défense particulièrement exposés.

La « protection fonctionnelle », est la protection, par la puissance publique, de ses agents dans l'exercice de leurs fonctions, en cas de mise en cause par des tiers. Ce soutien exprime un rapport de solidarité entre l'agent et son administration et ce, dans l'intérêt du service. Il peut prendre la forme de la prise en charge des frais d'avocat, par exemple.

Le 1^o du présent article ajoute les concubins de militaires et partenaires de pacte civil de solidarité, aux côtés des conjoints, au titre des bénéficiaires de la protection fonctionnelle pour les attaques dont ils sont victimes du fait de la

profession de ces derniers, par analogie à ce qui est prévu pour les fonctionnaires civils.

Le 2° du présent article accorde aux ayants droit des militaires un avantage que les ayants droit de certaines autres professions à risque (en charge de la sécurité intérieure) avaient déjà obtenu en 2003 et que le projet de loi relatif à la déontologie et aux droits et obligations des fonctionnaires adopté par le conseil des ministres du 17 juillet 2013 ⁽¹⁾ prévoit d'étendre aux ayants droit des fonctionnaires civils. Il dispose que le conjoint, concubin ou partenaire de pacte civil de solidarité, à défaut, les enfants agissant conjointement, et, à défaut, les ascendants agissant conjointement du militaire victime d'une atteinte volontaire à sa vie du fait de ses fonctions mais hors le cas d'une action de combat bénéficient également de la protection de l'État pour les instances qu'ils décideraient d'engager contre l'auteur de l'atteinte.

*

* *

*La Commission émet un avis **favorable** à l'adoption de l'article 22 **sans modification**.*

*La Commission émet un avis **favorable** à l'adoption de l'ensemble des dispositions dont elle s'est saisie, sous réserve des **modifications** apportées par les amendements qu'elle a adoptés.*

M. le président Jean-Jacques Urvoas. Je constate que la Commission a décidé à l'unanimité d'émettre un avis favorable. Monsieur le rapporteur, je vous félicite pour ce travail consensuel !

(1) Enregistré à la présidence de l'Assemblée nationale le 17 juillet 2013, doc. AN n° 1278.

PERSONNES ENTENDUES PAR LE RAPPORTEUR POUR AVIS

- **Secrétariat général de la défense et de la sécurité nationale**

- M. Francis Delon, secrétaire général de la défense et de la sécurité nationale
- Mme Agnès Deletang, conseillère des affaires juridiques
- M. Marc Antoine, conseiller pour les relations institutionnelles et la communication

- **Communauté du renseignement**

- M. le général de corps d'armée Jean-Pierre Bosser, directeur de la protection et de la sécurité de la Défense
- M. Jean-Paul Garcia, directeur national du renseignement et des enquêtes douanières
- M. Bernard Bajolet, directeur général de la sécurité extérieure
- M. Jean-Baptiste Carpentier, directeur de la cellule TRACFIN (traitement du renseignement et action contre les circuits financiers clandestins)
- M. le général de corps d'armée Christophe Gomart, directeur du renseignement militaire