N° 2691

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 31 mars 2015.

AVIS

FAIT

AU NOM DE LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES
SUR LE PROJET DE LOI (n° 2669),
relatif au **renseignement**,

PAR M. PHILIPPE NAUCHE,

Député.

Voir les numéros :

Assemblée nationale : **2697.**

SOMMAIRE

___

Pages

INTRODUCTION

Le Livre blanc sur la défense et la sécurité nationale de 2013 a réaffirmé, dans la continuité de la programmation militaire précédente, que la fonction « connaissance et anticipation » était un élément fondamental de la stratégie de sécurité nationale et la condition de « décisions libres et souveraines ».

Le projet de loi sur le renseignement vient parachever les importantes réformes entreprises depuis 2008 pour doter la France de capacités techniques, humaines et financières en matière de renseignement en adéquation avec les enjeux stratégiques contemporains.

Il ne s'agit en effet pas d'une loi de circonstance, dictée par l'émotion suscitée par les attentats meurtriers des 7, 8 et 9 janvier derniers. Elle est plutôt le fruit d'un travail engagé depuis plusieurs mois par le Gouvernement et le Parlement, appuyé par les travaux tant de la commission des Lois que de la délégation parlementaire au renseignement, dont elle reprend l'essentiel des propositions.

Ce projet de loi vise à combler les lacunes d'une législation éparse, dont certaines dispositions étaient entrées en vigueur il y a plus de vingt-cinq ans, bien avant l'explosion des communications téléphoniques et des réseaux électroniques de télécommunications. Il permettra de doter les services de renseignement d'outils techniques adaptés à ces évolutions technologiques et aux mutations de la menace.

Surtout, ce projet de loi permet de définir, pour la première fois, une véritable politique publique de renseignement, et de la doter d'un cadre juridique clair et stable, à la fois plus protecteur pour les agents de ces services et pour l'ensemble des citoyens.

La protection des libertés individuelles ne doit en effet pas être sacrifiée sur l'autel de la lutte contre le terrorisme. Le projet de loi organise pour cela un contrôle très strict des activités de renseignement grâce à un cadre contraignant, des procédures lisibles, une autorité administrative indépendante aux pouvoirs renforcés et un contrôle juridictionnel inédit.

Le texte présenté par le Gouvernement est donc un texte équilibré, tant par les droits nouveaux qu'il accorde aux services que par les garanties qu'il offre, en contrepartie, aux citoyens. Après avoir adopté quelques amendements de précision du rapporteur, en matière notamment de protection pénale des agents et de respect du secret de la défense nationale lors des procédures contentieuses, la commission de la Défense a émis un avis favorable à l'adoption de ce projet de loi.

I. LA CONSÉCRATION LÉGISLATIVE D'UNE POLITIQUE PUBLIQUE DE RENSEIGNEMENT

Le projet de loi a pour ambition de donner un cadre juridique clair et unifié aux activités des services de renseignement et de faire ainsi sortir de l'ombre une politique publique qui émerge véritablement depuis quelques années seulement.

A. UN CADRE D'ACTION STRICTEMENT DÉFINI

Le Livre blanc sur la défense et la sécurité nationale de 2013 a conforté et amplifié l'effort entrepris par le Livre blanc de 2008, qui avait fait de la nouvelle fonction « connaissance et anticipation » une priorité de la stratégie nationale de défense et de sécurité.

Depuis 2009, il a été ainsi entrepris une importante réorganisation de la gouvernance des services de renseignement qui a permis de constituer une « communauté du renseignement ». Celle-ci est organisée autour d'une nouvelle coordination nationale, assurée par un Conseil national du renseignement, présidé par le Président de la République. Pour *« coordonner l'action et s'assurer de la bonne coopération des services spécialisés constituant la communauté française du renseignement »*, une fonction de coordonnateur national du renseignement a été créée dans le même temps [(1)].

Ce dernier réunit autour de lui, au moins une fois par mois, les six chefs de services spécialisés :

– la direction générale de la sécurité extérieure (DGSE) ;

– la direction du renseignement militaire (DRM) ;

– la direction de la protection et de la sécurité de la défense (DPSD) ;

– la nouvelle direction générale de la sécurité intérieure (DGSI) ;

– la direction nationale du renseignement et des enquêtes douanières (DNRED) ;

– le service de traitement du renseignement et de l'action contre les circuits financiers clandestins (TRACFIN).

Mieux identifiée et mieux coordonnée, la communauté du renseignement a parallèlement entrepris un effort important de modernisation de ses équipements, permettant à la France de combler une partie du retard pris sur ses principaux partenaires. La loi de programmation militaire

(1) Article R. 1122-8 du code de la défense.

pour les années 2014 à 2019 prévoit ainsi la poursuite de la réalisation de programmes d'équipements majeurs lancés au cours de la précédente programmation et donne la priorité aux composantes spatiales et aériennes, pour l'imagerie et l'interception électromagnétique. Le rapport annexé au projet de loi de programmation précisait ainsi que *« le développement de nos capacités de recueil, de traitement et de diffusion du renseignement [serait] prioritaire sur toute la durée de la planification. »*

Le Livre blanc de 2013 a également rappelé le rôle de pilotage stratégique que doit assurer le Conseil national du renseignement et prévu que celui-ci arrête désormais une stratégie nationale du renseignement, document de référence appelé à être rendu public, dont les plans nationaux d'orientation du renseignement (PNOR) constituent les déclinaisons opérationnelles.

Le projet de loi consolide ces évolutions et définit, pour la première fois dans un texte législatif, les missions assignées aux services de renseignement.

Ces missions, définies par l'article 1er du projet de loi (**nouvel article L. 811-2 du code de la sécurité intérieure**), fixent le cadre général dans lequel les services doivent inscrire leur action. N'y sont pas seulement mentionnées la prévention de risques et de menaces mais aussi la connaissance des enjeux géopolitiques et stratégiques, ce qui traduit bien les deux volets de leur action, à la fois défensive et prospective. Ce même article inscrit la politique de renseignement dans le cadre de l'action du Gouvernement et consacre au niveau législatif le Conseil national du renseignement.

Le projet de loi décline ensuite les motifs justifiant le recours aux techniques de renseignement qu'il prévoit.

En application du principe de proportionnalité (**nouvel article L. 811-1**, **introduit par l'article 1er**), ces techniques, par nature intrusives, ne pourront être utilisées qu'à condition que d'autres sources de renseignement – renseignement humain, sources « ouvertes » – ne puissent fournir le renseignement recherché. Elles ne couvrent donc qu'un champ de l'activité des services, leurs modes d'action étant plus diversifiés que l'usage de ces dites techniques.

Les motifs de recours à celles-ci sont décrits avec la plus grande précision. Cela est fondamental car c'est au regard de ces finalités que l'autorité administrative indépendante chargée de donner un avis préalable à l'autorisation de mise en œuvre appréciera la pertinence de la demande, ainsi que le fait aujourd'hui la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Le projet de loi (**nouvel article L. 811-3, article 1er**) dresse une liste de sept finalités justifiant le recours à des techniques de renseignement. L'actualisation des cinq motifs prévus par la loi du 10 juillet 1991 sur les interceptions de sécurité était rendue indispensable pour tenir compte tant de la

« jurisprudence » élaborée par la CNCIS au cours de ces vingt-cinq dernières années que pour traduire le plus fidèlement possible la réalité des missions des services de renseignement. Les sept finalités prévues par le projet de loi reprennent donc les cinq motifs de la loi de 1991 en y ajoutant la prévention des violences collectives et les intérêts essentiels de la politique étrangère.

B. DES OUTILS NOUVEAUX, ADAPTÉS AUX ÉVOLUTIONS DE LA MENACE ET AUX MUTATIONS TECHNOLOGIQUES

En dépit des efforts importants réalisés depuis la parution du Livre blanc de 2008, le cadre juridique dans lequel les services de renseignement exercent leur activité est encore insuffisant sur plusieurs points pour leur permettre de répondre efficacement aux défis auxquels ils sont confrontés.

Si la loi de programmation militaire pour les années 2014 à 2019 a permis d'étendre l'accès des services de renseignement à certains fichiers et rénové le cadre juridique de la géolocalisation en temps réel, ces services ne disposent en effet pas de moyens d'investigation comparables à ceux qui ont été accordés aux services de la police judiciaire ces dernières années. Outre l'accès à certains fichiers, seuls deux viatiques leur sont aujourd'hui offerts : les interceptions de sécurité – les « écoutes téléphoniques » – dans le cadre de la législation adoptée en 1991, et l'accès à l'ensemble des données techniques de connexion, depuis 2006.

Conformément aux propositions formulées par la délégation parlementaire au renseignement dans son rapport d'activité pour 2014, **le projet de loi transpose dans le domaine administratif certaines techniques utilisées par la police judiciaire** : la pose de balises (**nouvel article L. 851-6, introduit par l'article 2)** et la captation d'images, de sons ou de données informatiques, le cas échéant avec intrusion domiciliaire (**nouveaux articles L. 853-1 et L. 853-2, introduits par l'article 3**).

Il crée également deux nouveaux modes d'exploitation des données de connexion, c'est-à-dire des données techniques permettant d'identifier les numéros d'appareils mobiles et de connexion à un serveur, la liste des numéros appelés et la durée des conservations. L'explosion des communications mobiles constatée depuis vingt-cinq ans et la diversification des réseaux et supports de communications électroniques exigent en effet l'usage de techniques plus sophistiquées que celles prévues par la loi 1991.

Le projet de loi créé ainsi la possibilité de suivre en temps réel, par le recueil de données de connexion, un groupe de personnes préalablement identifiées comme présentant une menace terroriste (**nouvel article L. 851-3, introduit par l'article 2**). Cela doit permettre d'opérer une surveillance plus efficace d'individus, recensés par les services et impliqués dans des filières terroristes, et d'établir les liens qu'ils pourraient tisser entre eux dans la préparation d'un acte.

Pour la seule prévention du terrorisme, il prévoit également la mise en place, directement sur les réseaux des opérateurs de télécommunications, des dispositifs techniques permettant de repérer des comportements suspects (**nouvel article L. 851-4, article 2**). Il s'agit d'identifier de nouveaux profils, sachant qu'aujourd'hui, seule la moitié des ressortissants français présents sur les zones de combat en Syrie avaient été préalablement identifiés par nos services.

Le projet de loi prévoit aussi le recours par les services à des « dispositifs techniques de proximité », c'est-à-dire des *IMSI-catchers*, appareils qui permettent de capter les données de connexion des appareils mobiles dans leur environnement immédiat (**nouvel article L 851-7, article 2**). Dans certains cas, et selon des conditions très strictes et pour une durée limitée, ces dispositifs pourront également servir à capter les correspondances émises.

Le régime des interceptions de sécurité évolue peu. Le projet de loi prévoit simplement la possibilité d'étendre le dispositif d'écoutes à l'entourage de la personne visée, ce que l'interprétation restrictive de la loi de 1991 faite par la CNCIS ne permet pas aujourd'hui (**nouvel article L. 852-1, article 2**). Les attentats commis en France en janvier dernier avaient en effet mis en lumière le rôle que peut jouer l'entourage des terroristes dans la préparation de leurs actes.

Enfin, le projet de loi créé **un cadre juridique spécifique pour les interceptions de communications électroniques émises ou reçues à l'étranger** (**nouvel article L. 854-1 introduit par l'article 3**). Il s'agit là de protéger les agents lorsqu'ils ont recours à une technique de renseignement visant un objectif étranger depuis le territoire national.

II. DES GARANTIES NOUVELLES POUR LA PROTECTION DES DROITS INDIVIDUELS

Contrepartie des pouvoirs nouveaux accordés aux services, les pouvoirs et les moyens de la nouvelle Commission nationale de contrôle sont renforcés et un véritable contrôle juridictionnel est instauré.

A. UNE PROCÉDURE D'AUTORISATION UNIQUE, SOUS LE CONTRÔLE D'UNE AUTORITÉ INDÉPENDANTE RENFORCÉE

Le projet de loi créé, tout d'abord, **une procédure d'autorisation unique, claire et lisible, pour toutes les techniques de renseignement**, là où il en coexiste aujourd'hui trois, pour les interceptions de sécurité, les données de connexion et la géolocalisation (**nouveaux articles L. 821-1 à L. 821-5, introduits par l'article 1er**). Cette autorisation sera délivrée par le Premier ministre, après avis préalable d'une autorité administrative indépendante, la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR) qui remplacera l'actuelle CNCIS.

Il s'agit d'un renforcement des prérogatives de cette dernière, qui ne connaît aujourd'hui que les interceptions de sécurité. Surtout, les avis de la Commission seront délivrés avant l'autorisation de mise en œuvre, et non plus après, comme le prévoyait la loi de 1991 – même si l'usage avait systématisé la pratique de l'avis préalable. Cela renforce, incontestablement, les garanties en matière de protection des libertés.

La procédure d'autorisation et le régime de conservation des données sont **gradués en fonction du caractère plus ou moins intrusif de la technique utilisée** :

– pour les données de connexion, l'autorisation sera délivrée pour une durée de quatre mois et les données pourront être conservées pendant cinq ans ;

– pour les interceptions de sécurité, l'autorisation sera délivrée pour quatre mois et les données conservées pendant un mois ;

– pour les « dispositifs techniques de proximité », l'autorisation sera délivrée pour quatre mois, ou six mois dans certains cas, la conservation des données pouvant être faite pendant cinq ans. Ces durées seront ramenées à seulement 72 heures pour l'autorisation et un mois pour la conservation si des correspondances sont captées ;

– pour la captation d'images, de données informatiques ou de sons, enfin, l'autorisation sera délivrée pour deux mois, la conservation des données sera autorisée pour douze mois et un mois seulement si des correspondances sont enregistrées.

TABLEAU SYNTHÉTIQUE DES PROCÉDURES APPLICABLES AUX TECHNIQUES DE RECUEIL DU RENSEIGNEMENT SUR LE TERRITOIRE NATIONAL

Techniques de renseignement (référence du nouvel article introduit dans le code de la sécurité intérieure par le projet de loi).	**Finalités justifiant le recours aux techniques**	**Durée de l'autorisation accordée**	**Durée maximale de conservation des données collectées**	**Particularités de la procédure** Droit commun : autorisation du Premier ministre après avis préalable de la CNCTR (L. 821-1) Urgence absolue : pas d'avis préalable de la CNCTR (L. 821-5)
*Données de connexion (L. 851-1)**	L. 811-3 (toutes)	4 mois	5 ans	-
*Données de connexion en temps réel (L. 851-5)**	L. 811-3 (toutes)	1 mois	5 ans	-
Liste d'individus identifiés (L. 851-3)	Prévention du terrorisme	4 mois	5 ans	-
Dispositif technique dans les réseaux (L. 851-4)	Prévention du terrorisme	4 mois	5 ans	-
Pose de balises (L. 851-6)	L. 811-3 (toutes)	4 mois	5 ans	En cas d'urgence liée à une menace imminente, pas d'autorisation du Premier ministre et d'avis préalable de la CNCTR
Dispositifs techniques de proximité pour données de connexion (L. 851-7 I)	L. 811-3 (toutes)	4 mois ou 6 mois	5 ans	Autorisation spécialement motivée si demande pour 6 mois
Dispositifs techniques de proximité pour correspondances (L. 851-7 II)	Prévention d'un acte de terrorisme	72 heures	1 mois	Autorisation spécialement motivée
*Interceptions de sécurité (L. 852-1)**	L. 811-3 (toutes)	4 mois	1 mois	-
Enregistrement images, sons, données informatiques à distance (L. 853-1)	L. 811-3 (toutes)	2 mois	12 mois et 1 mois pour correspondances	Si aucun autre moyen légal possible
Enregistrement images, sons, données informatiques avec intrusion domiciliaire (L. 853-2)	L. 811-3 (toutes)	1 mois	12 mois et 1 mois pour correspondances	Si aucun autre moyen légal possible Autorisation spécialement motivée Pas d'urgence absolue possible : avis de la CNCTR par tout moyen

* *Techniques déjà autorisées par l'actuel code de la sécurité intérieure.*

Le projet de loi crée **une procédure d'urgence absolue** où le Premier ministre pourra autoriser la mise en œuvre d'une technique sans l'avis préalable de la Commission (**nouvel article L. 821-5, article 1er**), sauf dans le cas de l'intrusion domiciliaire, où son avis sera toujours requis (**nouvel article L. 853-2, article 3**).

Le collège de la future Commission est renforcé puisqu'il passe de trois à neuf membres : quatre parlementaires assurant une représentation pluraliste, quatre magistrats ou anciens magistrats et une personnalité qualifiée dans le domaine des télécommunications (**nouvel article L. 831-1, article 1er**).

La Commission pourra assurer, comme le fait aujourd'hui la CNCIS, le contrôle de la mise en œuvre des techniques : la loi organise **un véritable droit d'information** à son profit, à chaque étape de la procédure (**nouvel article L. 833-1, article 1er**). Elle recevra ainsi les demandes et autorisations délivrées, pourra avoir accès à tous les registres, relevés, enregistrements et transcriptions de l'ensemble des techniques de renseignement, et pourra, enfin, demander à être informée à tout instant des modalités d'exécution des autorisations en cours. Elle pourra également accéder aux locaux des opérateurs de télécommunications (**article 6**).

La loi prévoit en outre que le Premier ministre sera chargé de définir les **modalités de la centralisation des renseignements collectés** et d'en assurer le respect (**nouvel article L. 822-1, article 1er**). Cette traçabilité et cette centralisation des données collectées sont indispensables à la bonne exécution du contrôle effectué par la nouvelle Commission. Quelles que soient les modalités d'organisation retenues par le Premier ministre, les règles fixées par la présente loi exigeront des services la mise en œuvre de procédures contraignantes et la création de cellules en mesure de fournir à la CNCTR l'ensemble des données nécessaires à son contrôle.

B. LA CRÉATION D'UN VÉRITABLE CONTRÔLE JURIDICTIONNEL

La loi met enfin en place, de façon inédite, un contrôle juridictionnel des activités de renseignement.

Sans préjudice éventuel de la saisine du juge pénal en cas d'irrégularité grave constatée par la CNCTR, la loi confie ce contrôle juridictionnel au Conseil d'État, juge naturel de l'administration dans l'exercice de ses prérogatives de puissance publique.

Si l'article 66 de la Constitution de 1958 dispose que l'autorité judiciaire est *« gardienne de la liberté individuelle »*, le Conseil constitutionnel considère en effet que cette compétence exclusive du juge judiciaire est limitée aux mesures de privation de liberté – la détention, la garde à vue ou encore l'hospitalisation sans consentement – c'est-à-dire au *« droit à ne pas être arbitrairement détenu »*. Les

techniques de renseignement ne constituant pas des mesures privatives de liberté, y compris, comme le souligne l'étude d'impact du projet de loi, *« lorsqu'elles impliquent une intrusion dans un lieu privé »,* leur contrôle juridictionnel ne saurait donc être réservé à l'autorité judiciaire.

Le Conseil d'État pourra être saisi de deux manières (**nouvel article L. 841-1, introduit par l'article 1er**) :

– par toute personne ayant un « intérêt direct et personnel », à condition d'avoir préalablement saisi la CNCTR ;

– par la CNCTR elle-même, si le Premier ministre n'a pas donné suite aux recommandations qu'elle lui avait faites après avoir estimé qu'une technique avait été irrégulièrement mise en œuvre.

La loi aménage la procédure applicable à ce contentieux, en dérogeant sur certains points au code de la justice administrative, pour concilier droit au recours effectif et exigences du secret de la défense nationale (**article 4**)

Une formation de jugement particulière du Conseil d'État sera ainsi appelée à connaître les affaires relevant de ce contentieux et ses membres seront habilités au secret de la défense nationale. Les exigences du contradictoire seront aménagées pour que le requérant n'ait pas accès à des informations couvertes par le secret de la défense nationale.

Si aucune illégalité n'a été commise, la décision informera le requérant sans, naturellement, confirmer ou infirmer la mise en œuvre d'une technique.

Si la formation de jugement constate une illégalité, elle pourra **annuler la décision** de mise en œuvre de la technique concernée et ordonner, le cas échéant, **la destruction des renseignements irrégulièrement collectés**. Elle pourra informer le requérant qu'une illégalité a été commise et **condamner l'État à indemniser le préjudice subi.**

Les dispositions ainsi introduites sont de nature à donner un poids accru à la CNCTR, dont les recommandations pourront être désormais suivies d'une sanction décidée par le juge administratif. En créant ce contrôle juridictionnel, le présent projet de loi renforce substantiellement la protection des droits des citoyens.

TRAVAUX DE LA COMMISSION

La commission examine pour avis, sur le rapport de M. Philippe Nauche, le projet de loi relatif au renseignement (n° 2669), au cours de sa réunion du mardi 31 mars 2015.

Un débat suit l'exposé du rapporteur pour avis.

M. Jean-Jacques Candelier. Je comprends la nécessité d'actualiser la loi de 1991. Toutefois, je m'interroge après que plusieurs organisations – *Privacy international*, *Amnesty international*, Fédération internationale des droits de l'homme, Ligue des droits de l'homme, Reporters sans frontières – ont fait part de leur vive inquiétude à l'égard d'un texte qui octroie un pouvoir de surveillance accru aux agences de renseignement. Celles-ci seraient ainsi autorisées à pirater les ordinateurs et autres appareils, à espionner les communications et à écouter toute personne ayant été en contact, même par hasard, avec une personne suspectée.

Le système de surveillance de masse que le projet de loi organise va à l'encontre des libertés individuelles, d'autant que les opérations de surveillance ne seront pas soumises au contrôle de l'autorité judiciaire, les autorisations étant données par le Premier ministre.

Certes, le projet de loi prévoit la création de la CNCTR mais ses avis ne sont pas très contraignants. En soustrayant au contrôle en amont des juges les activités de renseignement, le texte accroît les risques d'abus.

Je ferai connaître mon avis sur le texte adopté par la commission des Lois.

M. le rapporteur pour avis. Les articles de presse qui s'inquiétaient d'une surveillance de masse se rapportaient à une version du projet de loi antérieure à son examen par le Conseil d'État.

L'autorité judiciaire n'intervient pas car la prévention d'actes illégaux est du domaine de la police administrative. Les activités de renseignement se situent en amont ; elles visent à rassembler des éléments démontrant la préparation d'une infraction mais aucun délit n'a encore été commis, *a fortiori* aucune preuve recueillie. Si le travail de renseignement permet d'établir la commission d'infractions, on bascule alors dans le domaine judiciaire.

Quant aux craintes que vous exprimez sur l'efficacité de la CNCTR, cette dernière est une autorité administrative indépendante dont le niveau d'expertise sera comparable à celui de la CNIL, que personne ne songe aujourd'hui à remettre en cause. L'avis de la CNCTR représente une garantie pour les libertés publiques.

La CNCTR rendra un avis préalable sauf dans les cas d'extrême urgence. Pour la pose de balises en cas de menace imminente – l'un des rares cas dans lesquels il n'y a pas d'autorisation préalable –, l'exception est justifiée par l'opportunité matérielle de pouvoir installer cet équipement, qui n'est pas toujours compatible avec le temps de la consultation de la CNCTR. Celle-ci est toutefois informée immédiatement. Les écoutes en direction de l'étranger sont également soustraites à l'avis de la CNCTR. Toutefois, si ces écoutes renvoient à un identifiant français ou concernent un ressortissant français, la CNCTR est saisie de leurs modalités de conservation.

M. Jean-Jacques Candelier. Personne n'est à l'abri de contrôles et de caméras de surveillance. On laisse la place aux abus et aux bavures. La CNIL que vous avez citée a émis des réserves sur le texte.

M. le rapporteur pour avis. Je rappelle que les membres de la CNCTR, dont l'indépendance est garantie, sont fondés à saisir le Conseil d'État si le Premier ministre ne suit pas leurs recommandations.

Sont visées par le projet de loi au travers de la notion d'entourage les personnes directement en contact avec la personne surveillée. Là où d'autres agences étrangères retiennent une extension de la surveillance à « n +3 », le projet de loi la limite à « n +1 ». Jusqu'à présent, l'interprétation par la CNCIS de la loi de 1991 interdisait d'écouter l'entourage. Or, on sait que cette restriction a privé nos services d'un certain nombre de renseignements.

En outre, le groupement interministériel de contrôle (GIC) opère un tri dans les informations recueillies pour ne conserver que celles qui se rapportent au dossier. Les éléments relatifs à la vie privée ne sont pas retranscrits et sont détruits.

M. Philippe Folliot. Si le texte doit être replacé dans son contexte, il ne doit pas être dépendant de ce dernier. Il doit être pensé pour le moyen et long terme, même si l'émotion récente et la nécessité de faire face à des menaces terroristes toujours plus présentes et multiformes doivent être prises en considération.

Il convient de trouver le juste équilibre entre, d'une part, la nécessité de protéger notre pays, et d'autre part, l'impératif, tout aussi légitime, de garantir les libertés publiques, en se prémunissant contre les tentations d'utiliser un arsenal très intrusif à bien des égards à des fins qui s'éloigneraient de l'objectif initial. La société a besoin d'être protégée mais cette protection doit s'inscrire dans un cadre.

Le renforcement du contrôle et de l'évaluation des techniques utilisées et des résultats obtenus doit être le pendant des moyens donnés aux services de renseignement. Cette mission, qui dépasse le rôle de la CNCTR, revient au Parlement qui connaît déjà ces sujets au travers de la délégation parlementaire au renseignement.

M. Yves Fromion. Ce texte comporte des dispositions importantes et utiles pour le bon fonctionnement des services de renseignement. Je les approuve dans leur grande majorité.

Toutefois, je m'interroge sur la CNCTR. Je ne comprends pas pourquoi elle a été baptisée autorité administrative indépendante alors qu'elle est composée presque pour moitié de parlementaires. Ce mélange des genres me paraît malsain : soit il s'agit d'une commission parlementaire, soit il s'agit d'une autorité administrative indépendante, mais dans ce cas, que viennent faire les députés aux côtés de magistrats – et même de magistrats retraités –, voire sous l'autorité de ces derniers ? On peut certainement m'opposer des exemples probants. Mais je considère qu'on s'égare.

En outre, le Parlement exerce déjà une mission de contrôle de l'action administrative en matière de renseignement. Comment pourrait-il être à la fois juge et partie ?

Cette disposition fait tâche dans un projet de loi qui comporte par ailleurs des dispositions intéressantes et importantes.

Comment justifiez-vous cet objet particulier qu'est la CNCTR ?

M. Nicolas Dhuicq. Je suis sceptique sur la philosophie du texte : à force de vouloir préciser le réel dans la loi, celui-ci, parce qu'il est toujours en avance, risque de nous échapper. À force d'oublier qu'un État a besoin de zones d'ombre pour survivre, il est à craindre que chaque législature soit l'occasion de textes qui nient cette réalité.

L'alinéa 6 de l'article 2 fait référence aux seuls besoins du terrorisme et à des personnes préalablement identifiées. Ces précisions n'ont-elles pas pour conséquence de limiter le travail de renseignement ?

L'article 12 porte sur le renseignement pénitentiaire qui souffre de sous-effectifs et de sous-dotations. Une fois encore, les alinéas 4 et 6 me semblent par trop limitatifs au regard de l'objet du texte. Le rôle du service de renseignement pénitentiaire est restreint à la prévention des évasions ainsi qu'à la sécurité et au bon ordre des établissements, alors que le texte entend lutter contre les personnes dont l'objectif est de détruire l'État et la Nation. Le cloisonnement entre les services auquel on risque d'aboutir n'est pas bénéfique pour garantir la sécurité de notre pays.

Le texte reste donc selon moi à mi-chemin.

M. le rapporteur pour avis. Le texte ne fait pas suite aux attentats de janvier. Il est le fruit des travaux de la délégation parlementaire au renseignement et de la commission des Lois en vue de définir un cadre juridique pour l'action des services de renseignement que ces derniers réclament.

Je rappelle que le projet de loi liste sept motifs d'intérêt public qui justifient le recours à des techniques de renseignement, parmi lesquels la prévention du terrorisme. Pour les besoins de cette dernière, le projet de loi prévoit quelques dispositions particulières.

Quant aux personnes préalablement identifiées mentionnées à l'article 2, la CNCTR contrôle les mesures dont elles sont l'objet. Les techniques utilisées chez les opérateurs visent à repérer des comportements ou des usages permettant de penser que la personne se livre à des activités terroristes. Il ne s'agit pas d'un dispositif d'écoute de masse. Il n'est question ni de pêche à la ligne, ni de pêche au chalut. Les mesures sont très ciblées afin de préserver les libertés individuelles.

Le rôle de la délégation parlementaire au renseignement n'est pas de contrôler l'action quotidienne des services de renseignement – cette mission est dévolue à la CNCTR. La délégation contrôle l'action du gouvernement en matière de renseignement. Le Conseil constitutionnel a bien précisé en 2001 que les parlementaires n'avaient pas accès aux opérations en cours.

Monsieur Fromion, le mélange des genres est très répandu dans notre République. Il a cours à la CNIL et à la CNCIS. La présence de quatre parlementaires permet d'assurer une représentation pluraliste. En outre, ces derniers ont par définition une parole libre.

Le Gouvernement a souhaité la présence de parlementaires pour renforcer la protection des libertés publiques. Si le Premier ministre s'avisait de ne pas suivre de manière déraisonnable les recommandations de la Commission, les parlementaires seraient plus que d'autres capables de porter le fer.

Enfin, le texte prévoit une incompatibilité entre les fonctions de membre de la délégation parlementaire au renseignement et de membre de la CNCTR.

M. Yves Fromion. Puisque nous entrons sur un terrain nouveau, nous pourrions faire œuvre de purification en mettant fin au mélange des genres.

Le pluralisme ou les parlementaires ne sont pas en cause. Mais, pourquoi faire de cette Commission une autorité administrative ?

M. le rapporteur pour avis. En prévoyant la présence de parlementaires, le Gouvernement voulait également suivre les recommandations de la Cour européenne des droits de l'homme selon lesquelles cette présence constitue une garantie supplémentaire pour les citoyens.

Je rappelle que deux membres de la CNCTR ont la possibilité de saisir le Conseil d'État sur les mesures les plus attentatoires aux libertés. Les garanties existent.

La question du rôle du renseignement pénitentiaire est légitime. Il faut savoir que le ministère de la Justice ne souhaite pas que ce service devienne

membre de la communauté du renseignement. Aujourd'hui, le bureau du renseignement pénitentiaire s'en remet à la DGSI pour les affaires qui relèvent de la compétence de cette dernière. Je ne suis toutefois pas sûr que la Chancellerie maintiendra sa position à l'avenir.

M. Nicolas Dhuicq. Doit-on s'attendre dès lors à un nouveau texte ou à un changement de garde des Sceaux ?

M. le rapporteur pour avis. La Chancellerie est fidèle à une tradition qui dépasse les alternances.

Le bureau du renseignement pénitentiaire, qui a d'autres tâches à accomplir, préfère en quelque sorte sous-traiter ces affaires à la DGSI. Le statu quo s'explique peut-être par la volonté de ne pas introduire une instabilité supplémentaire dans un cadre juridique en construction.

M. Nicolas Dhuicq. Les établissements pénitentiaires sont une source importante de collecte de renseignements, l'actualité récente l'a montré. Faute d'évolution, nous risquons encore de perdre quantité de renseignements.

M. le rapporteur pour avis. La composition de la communauté de renseignement n'est pas du domaine législatif. Il est possible que, demain, le bureau du renseignement pénitentiaire intègre le deuxième cercle de la communauté de renseignement. Aujourd'hui la Chancellerie ne demande pas à bénéficier des techniques de renseignement auxquelles elle pourrait avoir accès en appartenant à ce cercle. Cette position est soutenue par la DGSI.

M. Joaquim Pueyo. Ce projet de loi répond à la nécessité d'adapter les techniques et les procédures mises à disposition des services de renseignement. Il me semble aller dans le bon sens pour lutter plus efficacement contre le terrorisme.

Les services de renseignement sont en première ligne pour contrer ceux qui souhaitent abattre notre vision commune d'une société ouverte et tolérante.

Je ne suis pas défavorable au recours à de nouvelles techniques, y compris les balises, micros et interceptions, d'autant que, parallèlement à ce dispositif, d'importantes garanties sont prévues pour les libertés publiques. Il n'est pas question de surveiller tout le monde dans un grand délire paranoïaque.

Toutefois, je souhaite insister sur la nécessaire indépendance de la future CNCTR qui sera la garante de la légalité des procédures et des libertés individuelles.

Pour la même raison, je souhaite connaître les garanties prévues pour la destruction des enregistrements et les moyens qui seront alloués à la Commission. Sans moyens, celle-ci ne pourra pas jouer son rôle de manière efficace.

La nomination des magistrats par les présidents des hautes cours nous assure que les futurs membres seront indépendants et épris de libertés individuelles, ceci pour répondre à notre collègue qui s'inquiétait d'une surveillance de masse.

M. Dhuicq a posé une bonne question sur l'article 12. Il faut absolument renforcer le renseignement pénitentiaire car il est une mine d'informations.

Face au scepticisme de certains de mes collègues, je salue la présence du procureur dans le dispositif. Les établissements pénitentiaires sont sous le contrôle de l'autorité judiciaire, ce qui constitue une autre garantie des libertés individuelles.

La maturité d'une société ne se reconnaît pas à sa capacité à opposer les grandes conceptions qui la fondent – libertés individuelles et collectives – mais à sa faculté à maintenir un équilibre précieux pour ne pas offrir aux obscurantistes les armes pour la mettre à bas.

M. Michel Voisin. Les écoutes sont sous-traitées à quatre sociétés – deux en région PACA, une en Rhône-Alpes et une en Île-de-France. Il y a quelques mois, la garde des Sceaux n'a pas daigné reconduire les conventions liant les ministères à ces sociétés. En conséquence, pendant huit jours, ces dernières ont suspendu leur activité mettant en panne l'appareil administratif.

Les conventions ont finalement été reconduites pour trente mois. Estimez-vous logique de prendre un tel risque quand on sait ce qui s'est passé quelques mois plus tard ?

Quelles garanties prévoit le texte si d'autres conventions devaient être signées ?

M. Gilbert Le Bris. Ce texte est nécessaire. Il y a dix ans déjà, je plaidais pour le nécessaire contrôle législatif du processus de renseignement ; notre pays était en retard par rapport aux autres pays développés.

Ce texte est utile car il parvient à trouver un équilibre entre la liberté et l'efficacité. Mais, comme tout texte législatif, suivant l'usage qui en sera fait, il penchera d'un côté ou de l'autre. Tout pouvoir peut se livrer à des interprétations, dans les limites du contrôle judiciaire.

Je regrette l'absence d'une disposition, bien qu'elle eût été considérée comme un cavalier législatif. Le secret des affaires n'est pas défini en droit français. Nous avions déposé une proposition de loi en juillet 2014 sur ce sujet qui fait figure de serpent de mer. Le projet de loi Macron a failli pallier cette lacune par voie d'amendement avant que les journalistes ne s'en émeuvent, à juste titre tant la rédaction était imparfaite. La disposition a été retirée. Elle ne figure pas non plus dans ce projet de loi. Or, une directive est en préparation sur le sujet. Il ne nous restera donc plus qu'à choisir ente adopter ou refuser la directive. J'aurais

préféré que nous soyons à l'initiative d'une évolution législative car nous n'avons pas aujourd'hui les moyens juridiques de protéger les informations stratégiques de nos entreprises qui sont mises à mal par des concurrents étrangers.

M. Olivier Audibert-Troin. Chacun s'accorde sur l'obligation de légiférer pour donner un cadre légal aux activités de renseignement.

La composition du CNCTR comporte deux membres du Conseil d'État, qui peuvent être en activité. Or, il se trouve que le Conseil d'État est aussi la voie de recours contre les décisions de la CNCTR. Comment les membres du Conseil d'État pourront-ils déjuger leurs collègues les plus éminents ?

Le commissaire aux droits de l'homme du Conseil de l'Europe a qualifié le projet de loi de faute sérieuse. *Amnesty International* a également émis des doutes. Dans une tribune récente, le syndicat de la magistrature a jugé ce texte liberticide au motif notamment qu'il refuse de consacrer un véritable contrôle *a priori*.

Compte tenu de ces prises de position, les recours contre les avis rendus par la CNCTR risquent d'être très nombreux. Or, le texte prévoit que les données collectées seront détruites à l'issue d'un délai de douze mois, sauf exceptions. Dans l'hypothèse très vraisemblable de recours devant la Cour européenne des droits de l'homme, ce délai vous paraît-il suffisant ?

Enfin, rien n'est prévu pour protéger les membres de la CNCTR contre d'éventuelles demandes de dommages-intérêts consécutives aux recours contre les avis de la Commission.

M. le rapporteur pour avis. La procédure de nomination des magistrats à la CNCTR fait intervenir les responsables des hautes juridictions, ce qui constitue une garantie.

À mon sens, le fait que le Conseil d'État soit à la fois la voie de recours et le corps d'origine de certains membres de la Commission n'est pas un obstacle. Des membres du Conseil d'État siègent dans toutes les autorités administratives. Cela n'empêche pas la haute juridiction de juger en toute indépendance.

S'agissant de la protection civile des membres de la CNCTR, la Commission ne rend pas des décisions mais des avis : la décision appartient au Premier ministre. C'est donc la responsabilité de l'État qui pourra être mise en cause. La seule chose que la CNCTR peut décider, c'est d'engager un recours contre une décision du Premier ministre.

Le texte cherche à trouver un équilibre entre l'efficacité nécessaire de nos services et la préservation des libertés publiques. M. Audibert-Troin, compte tenu de votre groupe politique, je trouve intéressant que vous citiez avec bonheur le syndicat de la magistrature.

Dans le monde du droit, deux conceptions s'opposent : pour certains, seul l'ordre judiciaire est le garant des libertés publiques. Mais le juge administratif l'est tout autant, sauf pour les mesures privatives de liberté comme l'a rappelé le Conseil constitutionnel. Le juge judiciaire sera appelé à intervenir si des délits étaient mis en évidence par les mesures de police administrative.

Nous savons que les juges judiciaires utilisent largement les techniques de renseignement, y compris pour surveiller des personnalités éminentes. La police administrative en la matière est beaucoup plus contrôlée.

Monsieur Voisin, vous évoquez le cas des écoutes judiciaires qui ne sont pas l'objet du texte. Les écoutes administratives ne sont pas sous-traitées ; elles sont exclusivement réalisées par le GIC que j'ai évoqué dans mon propos introductif.

M. Michel Voisin. Les juges antiterroristes ordonnent des écoutes judiciaires. Il est scandaleux que le pays ait été privé de ces écoutes pendant une semaine sur la décision du garde des Sceaux.

M. le rapporteur pour avis. Je sais qu'il est de bon ton de mettre en cause la garde des Sceaux chaque fois que l'occasion se présente.

Je répète que le texte concerne les seules écoutes administratives réalisées par les services de renseignement. Il n'y a pas matière ici à traiter des écoutes judiciaires.

La commission en vient à l'examen des articles du projet de loi dont elle s'est saisie pour avis.

EXAMEN DES ARTICLES

Article 1er

(art. L. 811-1 à L. 811-4 (*nouveaux*), art. L. 821-1 à L. 821-6 (*nouveaux*), art. L. 822-1 à L. 822-6 (*nouveaux),* art. L. 831-1 (*nouveau*), art. L. 832-1 à L. 832-5 (*nouveaux*), art. L. 833-1 à L. 833-6 (*nouveaux*) et art. L. 841-1 (*nouveau*) du code de la sécurité intérieure)

Dispositions générales, procédure applicable, Commission nationale de contrôle des techniques de renseignement et recours juridictionnel

Le présent article complète le code de la sécurité intérieure en y introduisant un livre VIII, exclusivement consacré au renseignement. Ce livre rassemblera toutes les dispositions relatives à cette politique publique en reprenant, en les adaptant, les dispositions du titre IV du livre II du même code, consacré aux interceptions de sécurité, et les dispositions nouvelles créées par le présent projet de loi.

La création d'un cadre juridique unifié des services de renseignement était un vœu exprimé par la délégation parlementaire au renseignement dans ses deux derniers rapports d'activité [(1)] tant il était devenu indispensable, pour une démocratie moderne, de sortir du *« maquis juridique »* [(2)] pour offrir un cadre d'action clair à ses services, à la fois adapté à l'évolution de la menace et aux mutations technologiques tout en assurant la nécessaire protection des libertés individuelles.

1. Dispositions générales

Le titre Ier de ce nouveau livre VIII, intitulé « Dispositions générales », fixe les principes et les finalités de la politique publique de renseignement. Il crée un cadre légal commun à toutes les techniques de renseignement, là où seules les interceptions de sécurité bénéficiaient, jusqu'à présent, d'une législation précise.

Le nouvel article L. 811-1 rappelle, tout d'abord, les exigences de respect de la vie privée, notamment le secret des correspondances et l'inviolabilité du domicile. Si ces droits sont déjà reconnus par des dispositions constitutionnelles et conventionnelles, cet article précise qu'il ne peut y être porté atteinte que *« dans les seuls cas de nécessité d'intérêt public prévu par la loi »,* conformément à la jurisprudence constante du Conseil constitutionnel et aux dispositions de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

---

(1) Délégation parlementaire au renseignement, rapport d'activité 2013 présenté par M. Jean-Pierre Sueur, sénateur, et rapport d'activité 2014 présenté par M. Jean-Jacques Urvoas, député.

(2) Rapport d'information n° 1022 de la commission des lois de l'Assemblée nationale sur l'évaluation du cadre juridique applicable aux services de renseignement, 14 mai 2013, p. 14.

Ce nouvel article consacre, pour la première fois, le principe de proportionnalité, c'est-à-dire que les atteintes à la vie privée doivent être appréciées au regard des finalités poursuivies et que les techniques les plus intrusives ne doivent être utilisées qu'à condition que d'autres méthodes de renseignement ne puissent pas être employées pour parvenir aux mêmes fins. Ce principe se traduit dans la gradation, prévue par le projet de loi, des procédures d'autorisation, des durées d'utilisation et des durées de conservation des données en fonction du caractère plus ou moins intrusif des techniques utilisées.

La commission a adopté un amendement du rapporteur pour avis qui apporte une définition à la politique publique de renseignement, notion introduite dans l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires par la loi de programmation militaire pour les années 2014-2019 [(1)] sans que son contenu ne soit précisé. Cette définition fait référence à deux notions déjà clairement définies par le législateur : la stratégie de sécurité nationale, définie à l'article L. 1111-1 du code de la défense et les intérêts fondamentaux de la Nation, définis par l'article 410-1 du code pénal.

Le nouvel article L. 811-3 introduit dans notre législation le détail des missions confiées aux services chargés de mettre en œuvre la politique publique de renseignement.

Les services spécialisés de renseignement n'y sont pas nommés, le projet de loi préférant renvoyer leur désignation à un décret pris en application de l'ordonnance du 17 novembre 1958 précitée. Ce choix s'explique par la volonté du Gouvernement de préserver la souplesse nécessaire à l'organisation de ses services et de ne pas figer une communauté du renseignement à la constitution très récente.

Si la rédaction de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 issue de la loi n° 2007-1443 du 9 octobre 2007 – qui avait créé la délégation parlementaire au renseignement – mentionnait les *« services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget »*, la rédaction résultant de la loi de programmation militaire pour les années 2014-2019 fait en effet seulement référence aux *« services spécialisés de renseignement désignés par décret »*.

Ce décret a été pris le 12 mai 2014 et est codifié à l'article D. 1122-8-1 du code de la défense. Il désigne les six services suivants :

– la direction générale de la sécurité extérieure (DGSE) ;

– la direction du renseignement militaire (DRM) ;

– la direction de la protection et de la sécurité de la défense (DPSD) ;

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

– la direction générale de la sécurité intérieure (DGSI) ;

– la direction nationale du renseignement et des enquêtes douanières (DNRED) ;

– le service de traitement du renseignement et de l'action contre les circuits financiers clandestins (TRACFIN).

Ce même article D. 1122-8-1 dispose que ces services *« forment avec le coordonnateur national du renseignement et l'académie du renseignement la communauté française du renseignement ».*

Le projet de loi décrit ensuite les missions assignées aux services de renseignement. Ce faisant, il fait sortir cette politique publique de l'ombre qui avait entouré sa création par étapes successives et permet de rompre avec la *« démarche elliptique »* (1) qui avait prévalu jusque-là. Les missions définies par l'article fixent le cadre général dans lequel les services doivent inscrire leur action. N'y sont pas seulement mentionnés la prévention de risques et de menaces mais aussi la connaissance des enjeux géopolitiques et stratégiques, ce qui traduit bien les deux volets de leur action, à la fois défensive et prospective.

L'article inscrit enfin cette politique dans le cadre de l'action du Gouvernement et consacre au niveau législatif le conseil national du renseignement, créé par le décret n° 2009-1657 du 24 décembre 2009 et codifié à l'article R. 1122-6 du code de la défense.

Aux termes de cet article, le conseil national du renseignement *« définit les orientations stratégiques et les priorités en matière de renseignement. Il établit la planification des moyens humains et techniques des services spécialisés de renseignement. »* Y siègent, sous la présidence du président de la République, le Premier ministre, les ministres et les directeurs des services spécialisés de renseignement dont la présence est requise par l'ordre du jour, ainsi que le coordonnateur national du renseignement.

Le nouvel article L. 811-3 décline les motifs justifiant de recours aux techniques de renseignement. Le champ de ces motifs est plus restreint que celui des missions assignées aux services par le précédent article.

Il s'agit en effet là de justifier le recours à des techniques attentatoires au respect de la vie privée. En application du principe de proportionnalité introduit par l'article L. 811-1, ces techniques ne peuvent être utilisées qu'à condition que d'autres sources de renseignement – renseignement humain, sources « ouvertes » – ne puissent fournir le renseignement recherché. Le présent article ne couvre donc qu'un champ de l'activité des services, leurs modes d'action étant plus diversifiés que le seul usage des techniques prévues par le projet de loi.

(1) Rapport d'activité 2014 de délégation parlementaire au renseignement, p. 68.

Puisque ces techniques sont intrusives, leur finalité doit être décrite avec la plus grande précision. Car c'est bien au regard de ces finalités que l'autorité indépendante chargée de donner un avis préalable à l'autorisation de mise en œuvre appréciera la pertinence de la demande. La Commission nationale de contrôle des interceptions de sécurité (CNCIS) effectue aujourd'hui sur ce point un contrôle très précis des finalités prévues par l'actuel article L. 241-2 du code de la sécurité intérieure. Elle écrit ainsi dans son dernier rapport d'activité que *« l'atteinte exceptionnelle à la vie privée qu'autorise la loi ne peut être justifiée […] que par la menace directe ou indirecte, actuelle ou future que la personne écoutée est susceptible de représenter […]. En l'absence de menace, et quel que soit l'intérêt que représente la cible comme source de renseignement pour le domaine considéré, l'atteinte à la vie privée serait contraire aux principes de proportionnalité et de subsidiarité. »* (1)

La loi se doit donc d'être la plus précise possible, ainsi que le rappelle la jurisprudence constante de la Cour européenne des droits de l'homme : *« Puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la loi irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'un tel pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire. »* (2)

Le projet de loi dresse une liste de sept finalités justifiant le recours à des techniques de renseignement. L'actualisation des cinq motifs prévus par l'article L. 241-2 du code de la sécurité intérieure – qui ne concernait que les interceptions de sécurité – était rendue indispensable pour tenir compte tant de la « jurisprudence » élaborée par la CNCIS au cours de ces vingt-cinq dernières années que pour traduire le plus fidèlement possible la réalité des missions des services de renseignement.

Quatre motifs sont identiques à ceux prévus par l'article L. 241-2 : la sécurité nationale, la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisées, la prévention de la reconstitution ou du maintien de groupements dissous.

Un motif, *« les intérêts économiques et scientifiques essentiels de la France »* est plus vaste que la précédente notion de *« sauvegarde des éléments essentiels du potentiel économique de la France »* dont la CNCIS fait une interprétation trop restrictive. La « jurisprudence » de la CNCIS la conduit en effet à ne délivrer d'autorisations que dans les cas précis de menace comme, par exemple, une *« intention de nuire aux intérêts d'une entreprise française »* (3). Or cette interprétation ne couvre qu'un champ de ce que l'on appelle le

(1) CNCIS, 22e rapport d'activité, 2013-2014, p. 117.
(2) CEDH, Malone c. Royaume-Uni, 2 août 1984.
(3) CNCIS, 22e rapport d'activité, 2013-2014, p. 115.

renseignement économique et financier, auquel la délégation parlementaire au renseignement a consacré une partie de son dernier rapport d'activité, et il était important que le législateur fasse preuve de plus de clarté sur ce point.

Deux motifs, enfin, apparaissent pour la première fois : *« la prévention des violences collectives de nature à porter gravement atteinte à la paix publique »,* et *« les intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France. »*

Les finalités ainsi définies couvrent l'intégralité de l'activité de renseignement des services utilisant les techniques entrant dans le champ de la loi. La commission a adopté deux amendements du rapporteur pour avis visant à élargir sensiblement le champ de ces finalités en substituant au mot : « essentiel », le mot « majeur » dans le cas de la politique étrangère et des intérêts économiques et scientifiques.

2. La procédure d'autorisation des techniques de renseignement

Le titre II, intitulé « De la procédure d'autorisation des techniques de recueil de renseignement », crée, pour l'ensemble des techniques, un régime unique d'autorisation de mise en œuvre, là où coexistent aujourd'hui trois procédures distinctes en fonction desdites techniques. Le chapitre I^{er} traite de l'autorisation de mise en œuvre.

Selon l'actuel article L. 242-1 du code de la sécurité intérieure, **les interceptions de sécurité** sont aujourd'hui proposées, de façon écrite et motivée, par les ministres de la Défense, de l'Intérieur ou chargé des douanes. L'autorisation est ensuite accordée par le Premier ministre, par décision écrite et motivée. Les ministres et le Premier ministre peuvent spécialement déléguer chacun deux personnes en charge de ces propositions et décisions.

Cette décision du Premier ministre fait l'objet, en l'état actuel du droit, d'un contrôle *a posteriori* de la CNCIS, autorité administrative indépendante.

L'actuel article L. 243-8 du code de la sécurité intérieure prévoit ainsi que les décisions du Premier ministre sont communiquées, dans un délai maximum de 48 heures, au président de cette institution. Si celui-ci estime que la légalité de cette décision *« n'est pas certaine »,* il réunit la Commission, qui statue alors dans les sept jours. Au cas où la Commission estime qu'une interception de sécurité a été autorisée en méconnaissances des dispositions légales, elle adresse au Premier ministre une recommandation *« tendant à ce que cette interception soit interrompue ».*

Si, formellement, la CNCIS est investie d'un simple pouvoir de recommandation *a posteriori* d'interruption d'écoutes déjà autorisées par le Premier ministre, ce pouvoir s'exerce, dans les faits, *a priori*. Avec le plein accord du Premier ministre, le pouvoir de recommandation s'est en effet transformé, dès les premiers mois de son fonctionnement, en un *« quasi-pouvoir de décision »*

selon les mots de l'ancien président de cette institution, Jean-Louis Dewost, dans son vingtième rapport d'activité [(1)], tant les avis de la Commission sont suivis par le pouvoir exécutif.

Cette pratique de l'avis *a priori* a été étendue, par décision de la Commission du 25 mars 2003, aux interceptions demandées en urgence absolue. Elle a été confirmée le 18 février 2008 par une directive du Premier ministre, qui a qualifié ce contrôle a priori de *« pratique la mieux à même de répondre à l'objectif de protection efficace des libertés poursuivi par le législateur »* [(2)].

L'accès aux **données de connexion** fait l'objet d'une procédure d'autorisation plus légère que celle des interceptions de sécurité.

Les demandes d'autorisation sont ainsi effectuées, selon les dispositions de l'actuel article L. 246-2 du code de la sécurité intérieure, directement par les agents des services, et non par leurs ministres de tutelle. Elles sont motivées mais la législation n'impose pas qu'elles soient écrites.

L'autorisation est accordée, non par le Premier ministre, mais par une personnalité qualifiée placée auprès de lui, ou par des adjoints qui peuvent la suppléer. L'avis de la CNCIS n'est sollicité à aucune étape de la procédure, ni avant la décision de la personnalité qualifiée, ni après. La CNCIS intervient en revanche dans la désignation de cette personnalité qualifiée puisqu'elle choisit un nom parmi la liste que lui soumet le Premier ministre. Elle est également destinataire du rapport d'activité ainsi que des décisions prises par la personnalité qualifiée.

L'autorisation de la **géolocalisation en temps réel** relève enfin d'un troisième régime, introduit dans le code la sécurité intérieure par un amendement parlementaire à la loi de programmation militaire pour les années 2014 à 2019 [(3)].

La procédure définie par l'article L. 246-3 du code de la sécurité intérieure est identique à celle applicable aux interceptions de sécurité. Les demandes d'autorisation sont effectuées par demande écrite et motivée des ministres intéressés et la décision est prise par le Premier ministre. Celui-ci communique sa décision au président de la CNCIS dans un délai de 48 heures. Comme pour les interceptions de sécurité, si celui-ci estime que la légalité de cette décision *« n'est pas certaine »*, il réunit la Commission, qui statue alors dans les sept jours.

Le nouvel article L. 821-1 aligne le régime d'autorisation de recueil des données de connexion sur celui des interceptions de sécurité : ce sera désormais le Premier ministre, ou l'une des personnalités spécialement déléguées par lui, qui délivrera l'autorisation, et non plus la personnalité qualifiée.

---

(1) CNCIS, 20e rapport d'activité, années 2011-2012, p. 12.

(2) Idem, *p. 56.*

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

Surtout, ce nouvel article légalise l'usage de l'avis préalable de la nouvelle Commission nationale de contrôle de technique des renseignements (CNCTR), appelée à se substituer à l'actuelle CNCIS. Comme le souligne cette dernière, « c*e contrôle* a priori *renforce les modalités de la protection de la correspondance privée. Il constitue une garantie importante en ce que l'avis de la Commission portant sur la légalité et sur la protection du secret des correspondances intervient avant la décision et la mise en œuvre de la mesure d'interception. »* (1)

Toutes les techniques de recueil du renseignement, sur le territoire national, prévues par le présent projet de loi – interceptions de sécurité, données de connexion, géolocalisation, localisation, sonorisation de certains lieux et véhicules et captation d'images et de données informatiques – seront soumises à l'avis préalable de la nouvelle CNCTR, sauf cas d'urgence absolue prévue par le nouvel article L. 821-5.

Ce faisant, **le projet de loi met en place une procédure unique, lisible et claire, et élargit les compétences de la CNCTR, alors que la CNCIS ne connaît aujourd'hui qu'un nombre limité de techniques de renseignement**. Il répond aux recommandations formulées de longue date par cette dernière, la délégation parlementaire au renseignement ainsi que par le rapport d'information de la commission des Lois précité.

Compte tenu de l'augmentation du nombre de techniques prévues par cette nouvelle procédure unique, l'article L. 821-1 prévoit de faire passer le nombre de personnes spécialement déléguées par le Premier ministre pour délivrer l'autorisation de deux à six.

Le nouvel article L. 821-2 encadre les demandes des services. Toutes les demandes devront être écrites et motivées – là où les demandes de recueil des données de connexion sont, par exemple, aujourd'hui simplement motivées.

Toutes les demandes seront également formulées par les ministres concernés, et non plus seulement par les agents comme c'est le cas actuellement pour les données de connexion. Les ministres pourront néanmoins déléguer auprès d'eux trois personnes chargées d'effectuer ces demandes, contre deux actuellement dans le cas des interceptions de sécurité.

Le nouvel article détaille enfin le contenu précis des demandes d'autorisation afin de permettre à la CNCTR d'effectuer un contrôle rigoureux de leur motivation et de leur justification.

Les demandes devront ainsi préciser la ou les techniques à mettre en œuvre, la ou les finalités poursuivies – finalités strictement définies par le nouvel article L. 811-3 – le ou les motifs des mesures, la ou les personnes, lieux ou véhicules concernés. Elles devront enfin préciser le service au bénéfice duquel elles sont présentées.

---

(1) CNCIS, 22e rapport d'activité, 2013-2014, p. 72.

Le nouvel article L. 821-3 détaille les modalités de recueil de l'avis de la CNCTR par le Premier ministre.

La demande de mise en œuvre est communiquée au président de la Commission, ou à un de ses membres désigné par lui. Il dispose alors de 24 heures pour rendre son avis au Premier ministre.

S'il estime que la validité de la demande du Premier ministre n'est pas certaine, le président de la CNCTR, ou le membre désigné par lui, réunit la Commission. Celle-ci doit alors rendre son avis dans un délai de trois jours ouvrables.

Si les avis ne sont pas rendus dans les délais prévus par le projet de loi – 24 heures ou trois jours – l'avis est réputé rendu.

Ainsi que le souligne l'étude d'impact du projet de loi, *« cette procédure allie les exigences opérationnelles, par sa rapidité […] et celles de la sécurité juridique »*.

Le nouvel article L. 821-4 encadre l'autorisation délivrée par le Premier ministre. Celle-ci sera, comme l'article L. 242-1 du code de la sécurité intérieure le prévoit aujourd'hui pour les interceptions de sécurité, écrite et motivée. Cela signifie que les données de connexion passeront désormais par une procédure écrite, là où la législation actuelle ne prévoit que la transmission d'un enregistrement des décisions, accompagnées de leur motif (actuel article L. 246-2 du code de la sécurité intérieure).

L'autorisation sera délivrée pour une durée initiale de quatre mois et sera renouvelable dans les mêmes conditions que l'autorisation initiale, ce qui correspond au régime actuel des interceptions de sécurité défini par l'article L. 242-3 du code de la sécurité intérieure. Néanmoins, pour certaines techniques particulières de recueil du renseignement, jugées plus intrusives, le projet de loi prévoit des durées d'autorisation plus courtes (*cf. ci-après les articles L. 851-5, L. 853-1 et L. 853-2*).

L'autorisation précisera la ou les techniques à mettre en œuvre, la ou les finalités poursuivies, le ou les motifs des mesures, le ou les lieux, véhicules ou personnes concernés. Dans ce dernier cas, les personnes pourront être désignées simplement *« par leurs identifiants ou leur qualité »* si elles ne sont pas nommément connues. L'autorisation précisera enfin le service autorisé à recourir à la technique de renseignement demandée.

Le registre des demandes et autorisations sera centralisé par les services du Premier ministre et sera tenu à la disposition de la CNCTR. Il s'agit là également d'un accroissement significatif de ses compétences, dans la mesure où elle n'a aujourd'hui accès qu'au registre des interceptions de sécurité et des données de connexion.

Le nouvel article L. 821-5 prévoit une dérogation à la procédure de recueil de l'avis préalable de la CNCTR avant la décision d'autorisation du Premier ministre. En cas d'urgence absolue, celui-ci pourra en effet autoriser directement le service à mettre en œuvre la technique concernée – sauf dans le cas des intrusions domiciliaires, où l'avis de la CNCTR sera toujours requis (*cf. ci-après, article L. 853-2).*

Ainsi que le précise l'étude d'impact du projet de loi, cette procédure *« n'a vocation à être utilisée qu'à titre exceptionnel »* et *« doit être motivée et réservée aux cas qui ne peuvent être anticipés et ne souffrent aucune attente (pose de balise, par exemple) »*. Même si la CNCIS réussit aujourd'hui à répondre dans des délais très brefs, parfois inférieurs à une heure, grâce à une permanence 24 heures sur 24, 365 jours par an, cet article doit laisser la possibilité au Premier ministre de donner son autorisation, en cas de menace imminente, dans un délai encore plus court.

Une procédure équivalente est prévue par l'article 230-35 du code de procédure pénale pour permettre à un officier de police judiciaire de mettre en place un dispositif technique sans autorisation du procureur de la République ou du juge d'instruction. Dans le cas de la police administrative, cette décision reviendra non pas à un agent des services mais au Premier ministre lui-même.

Le nouvel article L. 821-6 prévoit enfin la possibilité pour la CNCTR, une fois que l'autorisation aura été délivrée, d'adresser au Premier ministre une recommandation demandant d'interrompre la technique de renseignement mise en œuvre si elle estime que ladite autorisation a été délivrée en méconnaissance des dispositions prévues aux articles précédents.

Cette faculté figure déjà dans l'actuel article L. 243-8 du code de la sécurité intérieure mais la rédaction de ce nouvel article **ajoute la possibilité de demander la destruction des données collectées**. Surtout, elle introduit la possibilité pour la CNCTR de saisir le Conseil d'État si elle estime que le Premier ministre ne donne pas suite à ses recommandations ou si elle les juge insuffisantes (*cf. supra*).

3. Les renseignements collectés

Le chapitre II fixe les règles de conservation des renseignements collectés et les modalités de leur contrôle par la CNCTR.

Le nouvel article L. 822-1 définit tout d'abord les modalités de traçabilité des données collectées par les services de renseignement : chaque service devra établir un relevé mentionnant les dates de début et de fin de mise en œuvre ainsi que la nature des données collectées.

Il prévoit en outre que le Premier ministre sera chargé de définir les modalités de la centralisation des renseignements collectés et d'en assurer le respect.

Cette traçabilité et cette centralisation des données collectées sont indispensables à la bonne exécution du contrôle effectué par la CNCTR, ainsi que l'a souligné le président de l'actuelle CNCIS, M. Jean-Marie Delarue, lors de son audition par la commission de la Défense le 24 mars dernier. Actuellement, la centralisation des données est effectuée par un service technique, le groupement interministériel de contrôle (GIC), dont l'existence juridique repose sur le décret n° 2002-497 du 12 avril 2002. Ce service assure l'exécution des interceptions de sécurité pour le compte de l'ensemble des services de renseignement ainsi que, depuis début 2014, celle des données de connexion.

Comme le rappelle la CNCIS dans son dernier rapport d'activité, *« cette centralisation des moyens d'écoute, placés sous l'autorité du Premier ministre et confiés à un service technique neutre, puisqu'il n'est pas en charge de l'exploitation du renseignement et des enquêtes, a été considérée par le législateur comme une garantie fondamentale pour la protection des libertés publiques. »* (1)

En prévoyant ces exigences de traçabilité et de centralisation, les dispositions du présent article s'inscrivent pleinement dans cette philosophie.

Dans la mesure où certaines techniques de renseignement introduites par le présent projet de loi seront directement mises en œuvre par les services, et non plus par le seul GIC, les interlocuteurs du rapporteur lui ont indiqué qu'il pourrait être envisagé de déployer des cellules du GIC directement auprès des services, un peu à l'image des « GIC déconcentrés » qui ont été déployés sur le territoire national au plus près des services enquêteurs et dont la CNCIS a souligné l'utilité.

Il apparaîtrait en revanche imprudent, pour des questions évidentes de vulnérabilité que représenterait un tel système, de centraliser en un seul point toutes les données collectées par les services. Pour le contrôle de la mise en œuvre de certaines techniques, l'autorité indépendante devra donc se déplacer, comme elle a déjà pris l'habitude de le faire pour effectuer des contrôles inopinés ou programmés dans les services.

Quelles que soient les modalités d'organisation retenues par le Premier ministre, les règles fixées par la présente loi exigeront des services la mise en œuvre de procédures contraignantes et la création de cellules en mesure de fournir à la CNCTR ou aux agents du GIC l'ensemble des données nécessaires à leur contrôle.

Dans le même temps, afin de garantir l'effectivité de son contrôle, la nouvelle Commission devra se voir doter de moyens d'expertise technique renforcés. La commission de la Défense a adopté un amendement du rapporteur pour avis en ce sens.

Le nouvel article L. 822-2 fixe les règles de conservation des données collectées. Leur durée de conservation maximale est modulée en fonction de la

(1) CNCIS, 22e rapport d'activité, 2013-2014, p. 88.

technique utilisée : elle sera d'un mois, à compter de leur enregistrement – ou de leur déchiffrement si elles sont chiffrées – pour les interceptions de sécurité, de douze mois maximum pour les autres techniques et cinq ans pour les données de connexion. Un décret en Conseil d'État fixera précisément les durées de conservation de chacune de ces techniques.

Cette augmentation sensible des durées de conservation – les interceptions de sécurité étant actuellement détruites au bout de dix jours, les données de connexion après trente jours – trouve sa justification première dans l'augmentation spectaculaire des communications électroniques au cours des dernières années et d'une quantité d'informations à traiter sans commune mesure avec celle qu'on observait il y a vingt-cinq ans, au moment du vote de la loi de 1991 – 280 000 abonnés mobiles en France en 1994, 78,4 millions en 2014 d'après la CNCIS.

Dans de nombreux cas, les services doivent en outre recourir aux services d'un interprète pour des langues rares, ce qui n'est pas toujours compatible avec l'actuel délai de dix jours prévu pour les interceptions de sécurité. En outre, une analyse efficace des données collectées se fait souvent par un raisonnement itératif, qui nécessite pour cela de disposer d'un historique assez complet.

Une durée de conservation plus longue pourra être accordée aux données contenant des éléments de cyber-attaque afin de permettre aux services de conserver des échantillons de virus aux seules fins d'analyse technique.

Le nouvel article prévoit enfin que la CNCTR pourra, si elle estime que la conservation des données n'est pas effectuée selon les conditions fixées par le présent article, adresser une recommandation au Premier ministre et, le cas échéant, saisir le Conseil d'État dans les conditions fixées par le nouvel article L. 821-6.

Il convient enfin de préciser que la plupart du traitement des données se fait aujourd'hui selon un mode informatisé et automatisé, ce qui offre, selon les termes de la CNCIS, « *une garantie supplémentaire en termes de libertés publiques*. »

Le nouvel article L. 822-3 rappelle que les données ne peuvent être collectées, transcrites ou extraites qu'aux seules fins mentionnées au nouvel article L. 811-3. Il précise également que les transcriptions et extractions doivent être détruites si leur conservation n'est plus indispensable à ces mêmes finalités.

Les articles L. 822-4, L. 822-5 et L. 822-6 prévoient enfin la mise à disposition de la CNCTR des relevés de destruction des données collectées et la mise en œuvre des modalités de centralisation et de conservation des données sous l'autorité du Premier ministre.

4. La Commission nationale de contrôle des techniques de renseignement

Le titre III est consacré à la nouvelle Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante appelée à reprendre, avec des prérogatives renforcées, les compétences de l'actuelle Commission nationale de contrôle des interceptions de sécurité.

Le chapitre I[er] précise, tout d'abord, **sa composition.**

Pour répondre à l'augmentation des techniques de renseignement à disposition des services introduite par le présent projet de loi et à l'accroissement de son rôle dans la délivrance des autorisations de mise en œuvre, par la nouvelle procédure d'avis préalable, la composition de cette Commission est tout d'abord renforcée.

Le nouvel article L. 831-1 prévoit ainsi que ses membres passent de trois à neuf : deux députés et deux sénateurs, représentatifs du pluralisme du Parlement, deux membres ou anciens membres du Conseil d'État, deux magistrats ou anciens magistrats de la Cour de cassation et, fait nouveau, une *« personnalité qualifiée pour sa connaissance en matière de communications électroniques »*. Cette personnalité doit être à même de renforcer la compétence technique de la Commission afin de lui permettre d'exercer au mieux son contrôle sur les outils utilisés par les services de renseignement. Si la présence de parlementaires n'était pas forcément souhaitée par la délégation parlementaire au renseignement, la représentation de l'opposition au sein de la Commission est présentée comme une garantie d'indépendance renforcée au regard de la jurisprudence européenne en la matière.

L'indépendance des membres est garantie par leurs conditions de nomination : les noms seront proposés par les présidents des instances dont sont issus les futurs membres, le décret de nomination étant simplement « recognitif » comme c'est l'usage dans la nomination des membres d'autorités indépendantes.

Le mandat des membres, à l'exception de celui des parlementaires, sera de six ans, non renouvelable. Le président sera choisi parmi les membres issus du Conseil d'État ou de la Cour de cassation.

Les articles L. 832-1 à L. 832-5, introduits dans un chapitre II, fixent **les règles de déontologie et de fonctionnement de la Commission**. Y sont notamment précisés le régime des incompatibilités et les règles de quorum. Ils traitent également des moyens des services de la Commission, qui sera désormais dotée d'un secrétaire général et d'agents spécialement choisis *« en raison de leurs compétences juridiques, économiques et techniques en matière de communications électroniques et de protection des données personnelles »*. Le renforcement de ces moyens est indispensable, nous l'avons déjà dit, pour rendre son contrôle pleinement effectif.

Les articles L. 833-1 à L. 833-6 du chapitre III détaillent enfin **les missions** de la nouvelle Commission.

Le nouvel article L. 833-1 précise qu'elle devra veiller à la mise en œuvre des techniques de renseignement prévues par la loi.

Le nouvel article L. 833-2 organise un véritable droit d'information de la CNCTR, à chaque étape de la procédure. Elle recevra ainsi les demandes et autorisations délivrées, pourra avoir accès à tous les registres, relevés, enregistrements et transcriptions de l'ensemble des techniques de renseignement mentionnées au titre II, et pourra, enfin, demander à être informée à tout instant des modalités d'exécution des autorisations en cours.

Le Premier ministre pourra également lui communiquer tout ou partie des rapports de l'inspection des services du renseignement ainsi que des rapports des inspections des ministères, en lien avec les missions de la Commission.

Tel qu'il est rédigé, cet article offre des garanties importantes à la Commission et impose des règles contraignantes aux services.

Le nouvel article L. 833-3 permettra à la nouvelle Commission, comme le fait l'actuelle CNCIS, de procéder au contrôle de toute technique mise en œuvre, de sa propre initiative ou sur saisine de toute personne y ayant un intérêt direct et personnel.

Lorsqu'elle est saisie d'un simple soupçon de mise en œuvre d'une mesure de surveillance, elle procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect des dispositions légales et se borne à notifier à l'auteur de la réclamation qu'il a été *« procédé aux vérifications nécessaires »*, sans confirmer ni infirmer leur mise en œuvre.

À l'occasion de ces contrôles – 75 particuliers ont saisi par écrit la CNCIS en 2013 à cette fin – la Commission peut en effet découvrir les situations suivantes :

– existence d'une interception ordonnée par l'autorité judiciaire ;

– existence d'une interception de sécurité décidée et exécutée dans le respect des dispositions légales ;

– existence d'une interception de sécurité autorisée en violation de la loi ;

– existence d'une interception « sauvage », pratiquée en violation de la législation par une personne privée ;

– absence de toute interception.

On comprend aisément, au vu de ces différentes situations, *« que la Commission nationale n'a d'autre possibilité que d'adresser la même notification*

à l'auteur d'une réclamation, quelle que soit la situation révélée par les opérations de contrôle, et que toute autre disposition conduirait, directement ou indirectement, la Commission à divulguer des informations par nature confidentielles » ainsi que le soulignait le rapporteur de la loi de 1991 [(1)].

Outre que son contrôle portera désormais sur l'ensemble des techniques, et plus seulement sur les seules interceptions de sécurité, la nouvelle Commission pourra saisir le Conseil d'État, dans les conditions fixées à l'article L. 821-6, lorsqu'elle aura constaté une irrégularité.

Les articles L. 833-4 à L. 832-6 prévoient enfin, comme cela est déjà l'usage, la publication d'un rapport annuel d'activité de la nouvelle Commission ainsi que la possibilité d'adresser, à tout moment, des observations au Premier ministre et à la délégation parlementaire au renseignement. Elle pourra aussi répondre à des demandes d'avis du Premier ministre ou des présidents des assemblées parlementaires. Ainsi rédigés, ces articles confortent la place centrale qu'occupe l'autorité indépendante dans le contrôle des techniques de renseignement.

5. Les recours relatifs à la mise en œuvre des techniques de renseignement.

Le titre IV donne compétence au Conseil d'État pour exercer le contrôle juridictionnel de la mise en œuvre des techniques de renseignement.

En l'état actuel du droit, les citoyens peuvent contester la décision administrative autorisant la mise en œuvre d'une technique de renseignement ou saisir le juge pénal, si la mesure a été mise en œuvre en dehors de toute autorisation ou en méconnaissance de l'autorisation donnée.

Or, comme le souligne l'étude d'impact du projet, l'effectivité de ce contrôle est aujourd'hui limitée.

Tout d'abord, le juge administratif ne peut être saisi que d'une décision et, en l'état actuel du droit, seules les interceptions de sécurité et les données de connexion font l'objet de décision. En outre, le citoyen n'en a pas nécessairement connaissance.

Ensuite, les contrôles du juge administratif et du juge pénal sont limités par le secret de la défense nationale, qui couvre les opérations de recueil du renseignement. Seules les opérations préalablement déclassifiées peuvent être portées à leur connaissance pour leur permettre d'apprécier le caractère illégal ou non des interceptions en question.

L'idée du projet de loi est donc de **confier au Conseil d'État, de façon innovante, le contentieux de la régularité de la mise en œuvre des techniques**

(1) Assemblée nationale, rapport n° 2088 de François Massot, 6 juin 1991.

de renseignement. Cela doit permettre de *« concilier les exigences de confidentialité inhérentes au fonctionnement des services de renseignement avec le droit des citoyens, notamment au recours effectif »*, la haute juridiction bénéficiant pour cela de pouvoirs d'instruction accrus.

Le choix de la juridiction administrative, s'agissant de la mise en œuvre de techniques relevant de la police administrative – c'est-à-dire de la prévention, quand la police judiciaire a pour objet la répression – est tout à fait cohérent avec la *« conception française de la séparation des pouvoirs »*, telle qu'elle a été définie par le Conseil constitutionnel dans sa décision du 23 janvier 1987 : *« conformément à la conception française de la séparation des pouvoirs, figure au nombre des* "principes fondamentaux reconnus par les lois de la République" *celui selon lequel, à l'exception des matières réservées par nature à l'autorité judiciaire, relève en dernier ressort de la compétence de la juridiction administrative l'annulation ou la réformation des décisions prises, dans l'exercice des prérogatives de puissance publique, par les autorités exerçant le pouvoir exécutif »* [(1)].

Or, si l'article 66 de la Constitution de 1958 dispose bien que l'autorité judiciaire est *« gardienne de la liberté individuelle »*, le juge constitutionnel considère que cette compétence exclusive du juge judiciaire est limitée aux mesures de privation de liberté – la détention, la garde à vue ou encore l'hospitalisation sans consentement – c'est-à-dire au *« droit à ne pas être arbitrairement détenu »* [(2)].

Aussi, les techniques de renseignement ne constituant pas des mesures privatives de liberté, y compris, comme le souligne l'étude d'impact du projet de loi, *« lorsqu'elles impliquent une intrusion dans un lieu privé »*, leur contrôle juridictionnel ne saurait être réservé *« par nature »* à l'autorité judiciaire.

Le nouvel article L. 841-1 prévoit deux possibilités de saisine de la haute juridiction administrative :

– par toute personne ayant un *« intérêt direct et personnel »*, à condition d'avoir préalablement saisi la CNCTR dans les conditions fixées par l'article L. 833-3 ;

– par la CNCTR elle-même, si le Premier ministre n'a pas donné suite aux recommandations qu'elle lui avait faites après avoir estimé qu'une technique avait été irrégulièrement mise en œuvre.

« *L'intérêt direct et personnel* » constitue un mode de saisine assez large, proche de l'intérêt à agir de droit commun – sous la seule réserve qu'il sera réservé aux particuliers. Comme le précise l'étude d'impact, *« le simple soupçon étayé de la mise en œuvre d'une mesure de surveillance »* sera jugé suffisant.

---

(1) Décision n° 86-224 DC du 23 janvier 1987, considérant 15.
(2) Commentaires aux cahiers de la décision n° 2005-532 DC du 19 janvier 2006.

Le Conseil d'État pourra être également saisi à titre préjudiciel par toute juridiction administrative ou judiciaire saisie d'un litige dont la solution dépend de la régularité d'une technique de renseignement dont la mise en œuvre est alléguée.

Les modalités de mise en œuvre de ce nouveau contentieux sont précisées aux articles L. 773-1 à L. 773-7 introduits dans le code de la justice administrative par l'article 4 du présent projet de loi.

*

La commission est saisie de l'amendement DN1 du rapporteur pour avis.

M. le rapporteur pour avis. L'amendement vise à préciser que le renseignement est une politique publique qui concourt à la stratégie de sécurité nationale et à la sauvegarde des intérêts fondamentaux de la Nation. Il est ainsi fait référence à deux notions bien définies par le législateur : celle de stratégie de sécurité nationale, définie à l'article L. 1111-1 du code de la défense, et celle d'intérêts fondamentaux de la Nation, définie par l'article 410-1 du code pénal.

J'admets que cette disposition n'est pas de nature normative mais il me semble important de rappeler dans quel cadre s'exerce le renseignement.

*La commission **adopte** l'amendement.*

La commission examine, en présentation commune, les amendements DN2 et DN3 du rapporteur pour avis.

M. le rapporteur pour avis. Ces amendements proposent de substituer au terme « essentiels » celui de « majeurs » pour qualifier, d'une part, les intérêts de la politique étrangère et d'autre part, les intérêts économiques et scientifiques. En effet, la rédaction actuelle me semble trop restrictive. En outre, le caractère essentiel de ces intérêts peut évoluer dans le temps.

M. Nicolas Dhuicq. Je comprends la bonne intention du rapporteur. Mais l'argument temporel ne me semble pas recevable car le caractère essentiel est apprécié *in concreto*. Votre amendement illustre la contradiction interne du texte que j'évoquais précédemment qui tient à la primauté donnée à la lutte contre le terrorisme.

M. le rapporteur pour avis. L'alinéa 6 de l'article 2 que vous avez mentionné – limité, il est vrai, à la prévention du terrorisme – porte sur deux techniques seulement. L'ensemble des autres techniques de renseignement peuvent être utilisées pour les sept motifs listés par le projet de loi.

*La commission **adopte** les amendements.*

La commission est saisie de l'amendement DN4 du rapporteur pour avis.

M. le rapporteur pour avis. Cet amendement vise à faciliter la saisine du Conseil d'État dans les cas où la totalité des membres de la Commission ne serait pas en fonction, notamment à l'expiration des mandats des parlementaires et dans l'attente de la nomination de leurs successeurs à la Commission. Il ne faudrait pas que la saisine de la juridiction administrative soit empêchée par leur absence.

*La commission **adopte** l'amendement.*

La commission est saisie de l'amendement DN9 du rapporteur pour avis.

M. le rapporteur pour avis. Cet amendement précise que la Commission dispose des moyens humains et techniques nécessaires à l'accomplissement de sa mission ainsi que des crédits correspondants, dans les conditions fixées par la loi de finances.

*La commission **adopte** l'amendement.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 1er **ainsi modifié**.*

*

* *

Article 2

(art. L. 246-1 à L. 246-5 du code de la sécurité intérieure, art. L. 851-3, L. 851-4, L. 851-6, L. 851-7 et art. L. 852-1 (*nouveaux*) du code de la sécurité intérieure)

Techniques de recueil de renseignement : données de connexion et interceptions de sécurité

Le **I** du présent article crée, dans le code de la sécurité intérieure, un titre nouveau consacré aux techniques de renseignement soumises à autorisation.

Ce titre définira de manière exhaustive l'ensemble des moyens légaux d'investigation mis à disposition des services. Il rassemblera à la fois des dispositions existantes rénovées, notamment en matière d'interceptions de sécurité et d'accès administratif aux données de connexion, et des dispositions nouvelles, en matière de sonorisation de certains lieux, de captation de données techniques ou encore de localisation en temps réel d'objets ou de personnes.

Il comprendra quatre chapitres :

– un chapitre Ier, consacré aux données de connexion ;

– un chapitre II, consacré aux interceptions de sécurité ;

– un chapitre III, consacré à la localisation, la sonorisation de certains lieux et véhicules et à la captation d'images et de données informatiques ;

– un chapitre IV, portant sur les mesures de surveillance internationale.

L'ensemble de ces techniques de renseignement, à l'exception des mesures de surveillance internationale, sera soumis au régime commun d'autorisation préalable du Premier ministre, après avis de la CNCTR, introduit dans le code la sécurité intérieure par l'article 1er du présent projet de loi (articles L. 821-1 à L. 821-6).

Le **II** du présent article a trait aux **données de connexion**, dont les modalités d'accès administratif seront regroupées au sein du chapitre Ier du code de la sécurité intérieure.

Les données de connexion sont définies par l'actuel article L. 246-1 du code de la sécurité intérieure : il s'agit des données techniques permettant d'identifier des numéros d'abonnement ou de connexion à des serveurs, de recenser l'ensemble des numéros d'abonnement d'une personne désignée, de localiser les équipements terminaux utilisés ou encore de connaître la liste des numéros appelés avec leur date et leur durée. Ce sont donc des informations relatives au « contenant » par opposition aux interceptions de sécurité qui permettent de connaître le contenu des conservations.

Même si leur caractère intrusif est considéré de moindre ampleur que celui des interceptions de sécurité, le régime qui leur sera désormais applicable est aligné sur celui des interceptions de sécurité.

Ce chapitre qui leur est consacré comprendra d'une part, en les rénovant, les actuelles dispositions du chapitre VI du code de la sécurité intérieure (articles L. 246-1 à L. 246-5) introduits par la loi de programmation militaire 2014-2019 et, d'autre part, des dispositions nouvelles créées par le II du présent article.

Les **1°** et **2°** du II renumérotent les actuels articles L. 246-1 et L. 246-2 du code de la sécurité intérieure qui permettent aux services de recueillir, auprès des opérateurs de télécommunications, les données de connexion. La procédure faisant intervenir la personnalité qualifiée est supprimée, le régime d'autorisation étant désormais celui de droit commun, défini par l'article 1er du présent projet de loi.

Le **3°** met à disposition des services de renseignement **deux nouveaux modes d'exploitation des données de connexion**.

Ces deux nouveaux modes d'exploitation constituent une réponse directe aux attentats qui ont frappé la France les 7, 8 et 9 janvier derniers. Ces actes ont en effet témoigné de la nécessité de suivre de la façon la plus exhaustive possible les échanges électroniques que peuvent nouer, sur le territoire national, les individus représentant une menace terroriste. Un tel suivi doit permettre *« la détection précoce des projets à caractère terroriste »* et de renforcer ainsi *« l'efficacité de leur prévention »* selon les mots de l'étude d'impact du projet de loi.

Ainsi que l'a indiqué le coordonnateur national du renseignement, M. Alain Zabulon, lors de son audition par la commission de la Défense le 17 mars dernier, les services estiment à plus de 3 000 le nombre d'individus qui,

sur le territoire national, représentent, à des degrés d'intensité variable, une menace terroriste. *« Le grand défi des services de renseignement est de parvenir à détecter, parmi ces 3 000 individus, ceux qui sont susceptibles de passer à l'acte »* avait-il précisé.

Le nouvel article L. 851-3 vise à effectuer une surveillance renforcée de ces 3 000 individus en offrant la possibilité aux services de renseignement de recueillir auprès des opérateurs de télécommunications les données de connexion d'un ensemble de *« personnes préalablement identifiées comme présentant une menace »*, en temps réel.

Le recueil de ces données de connexion n'est possible aujourd'hui qu'*a posteriori*, dans les conditions prévues par les actuels articles L. 246-1 et L. 246-2 du code de la sécurité intérieure. Si l'exploitation des données ainsi communiquées par les opérateurs de télécommunications garde toute sa pertinence et est conservée par le présent projet de loi, elle ne permet pas de connaître en temps réel les liens qui se tissent au sein d'un groupe identifié d'individus.

Les attentats de janvier 2015 ont démontré l'importance qu'occupaient les filières dans la commission de ces actes et qu'il était fondamental d'en reconstituer l'arborescence, en temps réel, pour prévenir leur action. *« Savoir que tel individu s'est connecté à tel autre individu bien connu des services depuis des années est une information qui s'appelle un « signal faible », et le défi des services est d'être capable de détecter ces micro-informations qui, mises bout à bout, permettent de renseigner sur un éventuel projet d'attentat »* avait ainsi encore expliqué le coordonnateur national du renseignement à la commission de la Défense.

À la différence du recueil *a posteriori*, le recueil en temps réel ne pourra s'effectuer que pour les *« seuls besoins de la prévention du terrorisme »*, et non pour l'ensemble des intérêts publics mentionnés à l'article L. 811-3 créé par l'article 1er du présent projet de loi. Le régime d'autorisation sera celui de droit commun, précisé par l'article 1er du présent projet de loi.

Si le suivi exhaustif d'activistes déjà identifiés et répertoriés est renforcé par ce nouvel article L. 851-3, il importe également que les services disposent de moyens d'investigation étendus pour identifier les individus impliqués dans les filières terroristes. Les personnalités entendues par le rapporteur lui ont effet confié que seule la moitié des ressortissants français qui avaient rejoint les zones de combat en Syrie avaient été préalablement identifiés par les services de renseignement.

Alors que les modes de communication des terroristes, exploitant les possibilités offertes par la multiplication des réseaux et supports de communication électronique, sont de plus en plus sophistiqués, les services ne sauraient se reposer sur leurs seuls moyens humains pour recueillir, exploiter, traiter et analyser une quantité exponentielle de données techniques.

Le nouvel article L. 851-4 prévoit donc la possibilité, pour les services, d'imposer aux opérateurs de télécommunications la mise en place de dispositifs techniques capables, par un traitement automatisé des données de connexion, de révéler certains comportements caractéristiques des modes de communication utilisés par les terroristes.

Ainsi que le précise l'étude d'impact du projet de loi, il s'agit là de *« privilégier la recherche d'objectifs enfouis sous le maquis des réseaux de communication transnationaux »*. Il n'est donc pas question d'une surveillance généralisée, mais plutôt d'une surveillance spécialisée, ciblée sur quelques objectifs précis. *« L'objectif n'est pas de surveiller des comportements sociaux, tels que la fréquentation de telle ou telle mosquée par telle ou telle personne. Mais nous connaissons les techniques qu'emploient les djihadistes pour dissimuler leurs communications et échapper à toute surveillance : ce sont ces attitudes de clandestinité qu'il s'agit de détecter afin de prévenir des attentats, sans avoir à pratiquer une surveillance de masse »* avait par exemple expliqué le directeur général de la sécurité extérieure, M. Bernard Bajolet, lors de son audition du 24 mars dernier.

La mise en œuvre de tels dispositifs techniques sur les réseaux des opérateurs de communications ne pourra être effectuée que pour les *« seuls besoins de la prévention du terrorisme »*, à l'exclusion donc des autres intérêts publics mentionnés à l'article L. 811-3 créé par l'article 1er du présent projet de loi. L'autorisation de mise en place de ces dispositifs sera délivrée par le Premier ministre, après avis de la CNCTR.

Les données ainsi collectées par les dispositifs ne permettront pas l'identification des individus à l'origine des comportements détectés : le traitement automatisé sera en effet réalisé de façon anonyme.

C'est seulement si l'analyse de ces données révèle la présence d'une menace terroriste que le Premier ministre pourra autoriser la levée de cet anonymat. Cette autorisation sera délivrée dans les conditions de droit commun introduites par l'article 1er du présent projet de loi.

Lorsque la personne sera ainsi identifiée, les services pourront alors décider, ou non, de poursuivre leurs investigations par le recours à une interception de sécurité ou toute autre technique de recueil du renseignement, dans les conditions de droit commun fixées par la présente loi.

Le **4°** du présent article renumérote l'actuel article L. 246-3 du code de la sécurité intérieure, qui a trait à la géolocalisation en temps réel. Sans changer le fond de ce dispositif, introduit par la loi de programmation militaire pour les années 2014-2019, il harmonise son régime d'autorisation sur celui de droit commun prévu par l'article 1er du présent projet de loi. L'autorisation sera toutefois accordée pour seulement trente jours, contre quatre mois dans la procédure de droit commun.

Le **5°** du présent article introduit **deux nouvelles techniques de recueil de renseignement** dans le code de la sécurité intérieure.

Le nouvel article L. 851-6 prévoit la possibilité d'utiliser des dispositifs permettant de localiser en temps réel un véhicule ou un objet, autrement dit leur géolocalisation par la pose de balises.

Il s'agit là de la transposition, dans le domaine administratif, d'une technique déjà utilisée par les services de renseignement lorsqu'ils agissent dans le cadre judiciaire. Introduite à l'article 230-32 du code de procédure pénale par la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, elle permet aux agents des services de localiser, à tout moment, un individu ou un bien. Elle est aujourd'hui fréquemment utilisée *« par les services de police, de gendarmerie et des douanes dans les enquêtes, afin de venir en soutien d'une surveillance physique d'une personne ou d'un bien, ou pour établir, en temps réel, l'itinéraire et les fréquentations d'une personne »* [(1)].

En pratique, il existe deux techniques de géolocalisation en temps réel :

« - le suivi dynamique, en temps réel, d'un terminal de télécommunication permet, par la mise en œuvre d'une procédure spécifique, de localiser notamment un téléphone portable ;

« - l'utilisation d'un dispositif dédié (une balise), installé sur un objet ou un moyen de transport, permet de déterminer, en temps réel, la position d'un objet (véhicule, container) ou d'un individu. » [(2)]

Cette nouvelle technique pourra être utilisée par les services pour la prévention des atteintes aux intérêts publics mentionnés au nouvel article L. 811-3, et non les seuls besoins de la prévention du terrorisme.

L'autorisation de recourir à cette technique se fera selon la procédure de droit commun prévue à l'article 1er du projet de loi.

Néanmoins, l'article L. 851-6 prévoit la possibilité de déroger à cette procédure *« en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement »*. Il s'agit là de prévoir les rares cas où les agents ne disposeraient que d'un créneau de quelques minutes – voire de quelques secondes – pour poser la balise sur le véhicule ou l'objet.

Dans ce cas, la pose du dispositif pourrait se faire sans autorisation préalable du Premier ministre. Celui-ci serait alors informé sans délai, ainsi que la CNCTR. S'il ne délivre pas son autorisation dans les 48 heures, après avis de la CNCTR, le Premier ministre pourra *« ordonner la cessation immédiate du*

(1) Étude d'impact de la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.
(2) Idem.

dispositif et de l'exploitation des renseignements collectés, ainsi que la destruction de ces derniers ».

Le nouvel article L. 851-7 prévoit la possibilité, pour les services, de recourir à un « *dispositif technique de proximité* ».

Il s'agit de permettre aux services de renseignement, lorsqu'ils agissent dans un cadre préventif, d'utiliser ce que l'on appelle couramment des *IMSI-catchers* – pour *international mobile subscriber identity*, soit en Français, attrapeur d'identité internationale d'abonné mobile. Concrètement, ce sont des appareils de faible taille, interdits à la vente en France et que seuls certains services sont autorisés à posséder en vertu de l'article 226-3 du code pénal, qui permettent de récupérer les identifiants IMSI et IMEI (pour *international mobile equipement identity*) mais aussi, pour certains d'entre eux, d'intercepter les messages, appels téléphoniques et autres données envoyées par les téléphones mobiles situés à leur proximité.

La rédaction retenue par l'article L. 851-7 conduira les services à n'utiliser qu'une partie des potentialités offertes par ces équipements puisque seules les données de connexion strictement nécessaires à l'identification d'un téléphone mobile et leurs données techniques de localisation – soit les identifiants IMSI et IMEI – pourront être recueillies par les services.

Il ne s'agit donc en aucun cas de connaître le contenu des correspondances émises, qui aurait fait basculer l'usage de cette technique dans le régime des interceptions de sécurité. Seules les données de connexion, le « contenant », sera accessible aux services, ce qui justifie l'introduction de cet article dans le chapitre qui leur est consacré.

L'autorisation de recourir à ce dispositif interviendra selon la procédure de droit commun prévue à l'article 1er du projet de loi. Les équipements seront inscrits sur un registre spécial, qui pourra être vérifié par la CNCTR.

Par dérogation à la procédure de droit commun, cette autorisation pourra néanmoins être portée à six mois, au lieu de quatre habituellement. Dans ce cas, l'autorisation sera *« spécialement motivée et prise sur l'avis exprès »* de la CNCTR.

Enfin, et pour la seule prévention d'un **acte** de terrorisme, le dispositif technique pourra être utilisé pour intercepter directement des correspondances. Il s'agit là de prévoir des cas d'extrême urgence, où la commission d'un acte terroriste est imminente. Dans ce cas, l'autorisation sera délivrée dans les conditions de droit commun par le Premier ministre mais pour une durée limitée à 72 heures, et non plus de quatre mois. Les correspondances enregistrées devront être détruites dans un délai d'un mois, soit le régime applicable aux interceptions de sécurité.

Les **6°** et **7°** du présent article sont des articles de coordination.

Le **III** du présent article a trait aux **interceptions de sécurité**.

Le nouvel article L. 852-1 vise à se substituer aux actuels articles L. 241-2 et suivants du code de la sécurité intérieure, sans changer de manière substantielle le régime applicable aux interceptions de sécurité.

Les conditions de recours et la procédure d'autorisation seront celles de droit commun, précisées à l'article 1er du présent projet de loi.

La rédaction retenue introduit une nouveauté : la possibilité de recourir à des interceptions de sécurité sur *« l'entourage de la personne visée par l'autorisation »*. L'interprétation faite par la CNCIS de la législation actuelle la conduit en effet aujourd'hui à écarter cette faculté : *« une demande trop éloignée d'une implication directe et personnelle de la cible […] peut recevoir un avis négatif comme par exemple une demande où la démonstration de cette implication ne repose que sur un « relationnel » avec d'autres individus. »* (1)

Or l'efficacité de ces écoutes peut conduire les services à aller au-delà de la seule personne directement visée, *« un membre de son entourage immédiat étant susceptible de révéler des informations ayant un lien direct avec la poursuite des finalités assignées aux missions des services de renseignement »* selon les termes de l'étude d'impact du projet de loi.

La rédaction du nouvel article L. 852-1 vise donc précisément à lever l'ambiguïté de la législation actuelle et à autoriser les services à écouter également l'entourage direct des personnes visées. Elle prévoit cependant que cette autorisation ne sera délivrée qu'à condition que l'entourage en question soit *« susceptible de jouer un rôle d'intermédiaire, volontaire ou non »* ou de *« fournir des informations au titre de la finalité faisant l'objet de l'autorisation »*.

L'autorisation délivrée vaudra également autorisation de recueil des données de connexion.

Enfin, cet article rappelle les obligations de centralisation des données collectées, exécutées aujourd'hui par le groupement interministériel de contrôle, et la fixation du contingentement par le Premier ministre. Ce contingent, qui fixe le nombre maximum d'interceptions autorisées de manière simultanée, était de 2 190 en 2014, contre 1 180 en 1991 – ce qui témoigne d'une évolution raisonnable compte tenu de l'explosion concomitante des abonnés à un service de téléphonie. Ce quota oblige les services à se concentrer sur les cibles prioritaires, ce qui constitue une garantie pour les libertés publiques.

*

*La commission **adopte** l'amendement rédactionnel DN5 du rapporteur pour avis.*

---

(1) CNCIS, 20e rapport d'activité, 2011-2012, p. 62.

Elle est ensuite saisie de l'amendement DN6 du rapporteur pour avis.

M. le rapporteur pour avis. L'amendement prévoit la possibilité de renouveler l'autorisation de mise en œuvre du dispositif technique de proximité sur des lieux et pour des périodes déterminés, à l'instar de toutes les autres techniques de renseignement.

*La commission **adopte** l'amendement.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 2 **ainsi modifié**.*

*

* *

Article 3

(art. L. 853-1, L. 853-2 et L. 854-1 (*nouveaux*) du code de la sécurité intérieure)

Techniques de recueil de renseignement : localisation, sonorisation et captation d'images et mesures de surveillance internationale

Le présent article créé les deux derniers chapitres du titre V consacré aux techniques de renseignement soumises à autorisation.

Le chapitre III offre aux services **un nouveau mode de captation des données**.

Il étend en effet aux services de renseignement, conformément au vœu formulé par la délégation parlementaire au renseignement dans son dernier rapport d'activité, la possibilité de recourir à certains moyens d'investigation déjà utilisés par eux lorsqu'ils interviennent dans un cadre judiciaire, mais qu'ils ne peuvent utiliser lorsqu'ils agissent en matière de prévention [(1)].

Le nouvel article L. 853-1 prévoit le recours à des appareils enregistrant les paroles ou les images de personnes ainsi qu'à des logiciels captant leurs données informatiques. Il s'agit là de la transposition dans le domaine administratif de techniques utilisées dans le cadre de procédures judiciaires en vertu des articles 706-96 et 706-102-1 du code de procédure pénale.

Dans la mesure où l'atteinte à la vie privée est jugée plus attentatoire que le dispositif des interceptions de sécurité, l'autorisation ne pourra être délivrée, en application du principe de proportionnalité prévu par le nouvel article L. 811-1, que pour une durée initiale de deux mois, et non de quatre. Les correspondances et conversations enregistrées dans ce cadre devront être détruites dans un délai d'un mois, soit le régime applicable aux interceptions de sécurité. Les images et autres données pourront être en revanche conservées pendant une durée maximale de douze mois.

(1) Proposition n° 16 : transposer dans le domaine administratif certaines techniques spéciales de police judiciaire.

Le nouvel article L. 853-2 encadre strictement les conditions dans lesquelles la pose des appareils prévus par l'article précédent devra se faire en cas d'intrusion domiciliaire.

Selon le principe de proportionnalité, le recours à ces dispositifs ne pourra être autorisé que si les renseignements *« ne peuvent être recueillis par un autre moyen légalement autorisé. »*

L'autorisation sera délivrée selon les conditions de droit commun mais avec des garanties renforcées :

– la demande devra ainsi mentionner *« tous éléments permettant de justifier la nécessité de recourir à cette modalité ».* Elle devra mentionner le lieu, le propriétaire lorsqu'il est connu, ainsi que la nature du dispositif envisagé ;

– l'autorisation sera « *spécialement motivée* » et ne pourra être accordée que sur avis exprès de la CNCTR. Cela signifie que la procédure d'urgence absolue prévue par l'article L. 821-5, qui permet de se passer de l'avis préalable de la Commission, ne pourra en aucun cas être appliquée en cas d'introduction domiciliaire. L'article prévoit cependant qu'en cas d'urgence absolue, l'avis de la Commission et l'autorisation du Premier ministre pourront être accordés par *« tout moyen »*, c'est-à-dire sans nécessairement une procédure écrite ;

– enfin, l'autorisation ne sera délivrée que pour une durée maximale de trente jours, contre deux mois dans le cas de captation à distance et quatre mois pour les autres techniques de renseignement.

Tel qu'il est rédigé, cet article prévoit donc un cadre très strict, justifié par l'atteinte à la vie privée que représente une intrusion dans un lieu privé.

Le chapitre IV est consacré aux **mesures de surveillance internationale.**

Le nouvel article L. 854-1 créé un cadre juridique spécifique pour les interceptions de communications électroniques émises ou reçues à l'étranger.

La création d'un tel cadre faisait partie des recommandations de la délégation parlementaire au renseignement qui, dans son dernier rapport, soulignait que *« l'un des défis d'un prochain texte de loi résidera dans la prise en considération des activités déployées à l'étranger par certains de nos services – en particulier la DGSE. »* [(1)] Comme l'a souligné son directeur, M. Bernard Bajolet, lors de son audition devant la commission de la Défense le 24 mars dernier, cet article prend en considération les activités que mène la DGSE, sans y ajouter de capacités nouvelles. Il permettra ainsi de protéger les agents lorsqu'ils ont recours à une technique de renseignement visant un objectif étranger depuis le territoire national.

(1) Rapport d'activité 2014, p. 66.

Les conditions de recours à ces techniques seront les mêmes que celles prévues sur le territoire national, à savoir la protection des intérêts publics limitativement énumérés par l'article L. 811-3.

La procédure d'autorisation prévue par le présent article sera en revanche distincte puisque l'autorisation sera délivrée par le Premier ministre, sans avis préalable de la CNCTR. Cela est pleinement justifié par la nature des missions confiées à la DGSE – mais aussi à la DPSD ou à la DRM – qui concernent l'aspect le plus régalien de l'action de l'État à l'étranger, et dont l'appréciation ne saurait être confiée à une autorité administrative indépendante.

La CNCTR sera en revanche associée à la définition des conditions d'exploitation, de conservation et de destruction des renseignements collectés ainsi qu'à la procédure de délivrance des autorisations d'exploitation des correspondances, puisque le décret en Conseil d'État qui en précisera les modalités lui sera soumis pour avis.

Les modalités de mise en œuvre de ces mesures de surveillance seront précisées par un décret en Conseil d'État qui ne sera pas publié, comme cela est déjà l'usage pour certains décrets régissant les fichiers de souveraineté. Ainsi que le précise l'étude d'impact du projet de loi, *« leur divulgation dévoilerait en effet des informations de nature à porter gravement préjudice au secret de la défense nationale et à entraver les missions des services spécialisés de renseignement »*. Ce décret sera cependant soumis à l'avis de la CNCTR et porté à la connaissance de la délégation parlementaire au renseignement.

Si ces mesures de surveillance concernaient, de façon incidente, des personnes utilisant des identifiants français, les modalités de conservation et de destruction des données seraient celles de droit commun, définies par les articles L. 822-2 à L. 822-4 introduites par l'article 1er du projet de loi – à l'exception de leur délai d'exploitation, qui prendrait effet à compter de leur première exploitation, et non de leur enregistrement.

Enfin, la CNCTR sera chargée de veiller à ce que ces mesures de surveillance internationale par les services de renseignement soient mises en œuvre conformément aux décisions du Premier ministre. Elle fera, au moins chaque semestre, un rapport de son contrôle au Premier ministre qui sera alors tenu de répondre aux recommandations et observations qu'elle aura formulées.

*

*La commission émet un avis **favorable** à l'adoption de l'article 3 **sans modification**.*

*

* *

Article 4

(art. L. 311-4 *(nouveau)* et art. L. 773-1 à L. 773-7 (*nouveaux*) du code de la justice administrative)

Contentieux de la mise en œuvre des techniques de renseignement

Le présent article détaille les modalités de mise en œuvre du contrôle juridictionnel prévu par l'article le nouvel L. 841-1 du code de la sécurité intérieure introduit par l'article 1er du projet de loi.

Il aménage la procédure applicable à ce contentieux, en dérogeant sur certains points au code de la justice administrative, pour concilier droit au recours effectif et exigences du secret de la défense nationale.

Une formation de jugement particulière du Conseil d'État sera appelée à connaître les affaires relevant de ce contentieux et ses membres seront habilités au secret de la défense nationale. La commission de la Défense a adopté deux amendements du rapporteur pour avis visant à renforcer les exigences en matière de protection du secret de la défense nationale, dans la mesure où les affaires jugées devraient porter sur des opérations en cours : les affaires ne pourraient pas être portées à la section du contentieux ou à l'assemblée du contentieux et les membres appelés à juger de ces affaires devraient être habilités expressément, et non plus ès qualité, à connaître des informations classifiées.

Les exigences du contradictoire seront aménagées pour que le requérant n'ait pas accès à des informations couvertes par le secret de la défense nationale. En contrepartie, le Conseil d'État pourra soulever d'office tout moyen et demander à la CNCTR la communication de toutes les pièces nécessaires à l'instruction.

Si aucune illégalité n'a été commise, la décision informera le requérant sans, naturellement, confirmer ou infirmer la mise en œuvre d'une technique.

Si la formation de jugement constate une illégalité, elle pourra annuler la décision de mise en œuvre de la technique concernée et ordonner, le cas échéant, la destruction des renseignements irrégulièrement collectés. Elle pourra informer le requérant qu'une illégalité a été commise et condamner l'État à indemniser le préjudice subi.

Les dispositions ainsi introduites sont de nature à donner un poids accru à la CNCTR, dont les recommandations pourront être désormais suivies d'une sanction décidée par le juge administratif. En créant ce contrôle juridictionnel, le présent projet de loi renforce substantiellement la protection des droits des citoyens.

Enfin, si une illégalité commise est constitutive d'une infraction pénale, le Conseil d'État pourra saisir le procureur de la République.

*

La commission examine l'amendement DN8 du rapporteur pour avis.

M. le rapporteur pour avis. Compte tenu de la sensibilité des affaires qui y seront jugées et de l'autorisation qui sera donnée à ses membres d'accéder à l'ensemble des pièces en possession de la CNCTR et des services, la composition de la formation de jugement particulière doit être restreinte au strict nécessaire. L'amendement supprime également l'inscription des affaires au rôle de l'assemblée ou de la section du contentieux.

*La commission **adopte** l'amendement.*

La commission est saisie de l'amendement DN7 du rapporteur pour avis.

M. le rapporteur pour avis. Pour les mêmes raisons que précédemment, il est important de prévoir que les membres du Conseil d'État et les agents qui les assistent soient expressément habilités au secret de la défense nationale, là où le texte prévoit une habilitation ès qualité. L'amendement renforce le secret défense afin de maîtriser la diffusion des informations.

*La commission **adopte** l'amendement.*

*Puis elle émet un avis **favorable** à l'adoption de l'article 4 **ainsi modifié**.*

*

* *

Article 5

(art. L. 241-3, L. 241-4 et L. 242-9 du code de la sécurité intérieure, art. L. 861-4 (*nouveau*) du code de la sécurité intérieure)

Protection de l'anonymat des agents

Si les 1° à 4° du présent article sont des dispositions de coordination, le 5° introduit un nouvel article L. 861-4 dans le code de la sécurité intérieure. Il vise à mieux protéger l'anonymat des agents de services, comme le proposait la délégation parlementaire au renseignement, en supprimant ou en limitant l'obligation de publication des actes réglementaires et individuels qui leur sont relatifs.

Cette publication au *Journal officiel* des mesures d'organisation et des mesures nominatives constitue en effet une source de vulnérabilité pour les services et leurs agents. Les mesures nominatives seront désormais enregistrées dans un recueil spécial *« dispensé de toute publication ou diffusion et tenu par le Premier ministre »* selon les termes du deuxième alinéa de ce nouvel article.

Afin de garantir le contrôle du juge quant à l'opposabilité et la régularité des décisions, les troisième et quatrième alinéas prévoient une signature des actes par un numéro d'identification plutôt que par la mention des noms, prénoms et

qualité, et la communication au juge administratif des actes enregistrés dans le « recueil spécial » sans qu'ils ne soient versés au contradictoire.

*

*La commission émet un avis **favorable** à l'adoption de l'article 5 **sans modification**.*

*
* *

Article 6
(art. L. 244-1 à L. 244-3 du code de la sécurité intérieure, art. L. 871-4 *(nouveau)* du code de la sécurité intérieure)
Contrôle des réseaux des opérateurs de télécommunications par la CNCTR

Si les 1° à 5° sont des mesures de simple coordination, le 6° introduit un nouvel article L. 871-4 dans le code de la sécurité intérieure.

Ce nouvel article vise à autoriser les membres et les agents de la Commission nationale de contrôle des techniques de renseignement de pénétrer dans les locaux des opérateurs de télécommunications afin de contrôler la mise en œuvre des nouvelles techniques de renseignement créées par le présent projet de loi.

Si l'actuelle CNCIS dispose actuellement d'un accès direct aux données collectées par le groupement interministériel de contrôle pour le compte des services de renseignement, le contrôle qu'elle effectue n'est pas complet en l'absence d'un accès direct aux réseaux des opérateurs de télécommunications.

Cet article vise précisément à combler ce manque afin de renforcer l'étendue et l'efficacité des contrôles effectués par la CNCTR pendant et après la mise en œuvre des techniques de renseignement.

*

*La commission émet un avis **favorable** à l'adoption de l'article 6 **sans modification**.*

*
* *

Article 7
(art. L. 245-1 à L. 245-3 du code de la sécurité intérieure)
Coordination

Cet article est un article de coordination. Il déplace, en les adaptant, dans le nouveau livre VIII du code de la sécurité intérieure des dispositions pénales

existantes, qui répriment notamment le fait de révéler qu'une technique de renseignement est mise en œuvre ou le refus de transmettre des données de connexion dont le recueil a été autorisé.

*

*La commission émet un avis **favorable** à l'adoption de l'article 7 **sans modification**.*

*
* *

Article 8
(art. L. 895-1, L. 896-1, L. 897-1, L. 898-1 (*nouveaux*) du code de la sécurité intérieure)
Coordination

Cet article de coordination traite des conditions d'application outre-mer.

*

*La commission émet un avis **favorable** à l'adoption de l'article 8 **sans modification**.*

*
* *

Article 9
(art. L. 561-26 du code monétaire et financier)
Extension du droit de communication de TRACFIN

Cet article vise à renforcer le droit de communication de TRACFIN en l'étendant aux entreprises de transport ou des opérateurs de voyage et de séjour.

Pour remplir sa mission de lutte contre le blanchiment et le financement du terrorisme, TRACFIN dispose aujourd'hui de la faculté de demander, auprès des organismes financiers et autres professionnels concernés par le dispositif anti-blanchiment, tous les documents utiles à son enquête (relevés de comptes, factures, etc...) en vertu de l'article L. 561-26 du code monétaire et financier. Il peut également exercer ce droit de communication auprès des administrations d'État, des collectivités locales, des établissements publics ainsi que de toute personne chargée d'une mission de service public.

Le dispositif proposé complète l'article L. 561-26 précité afin de permettre à TRACFIN d'exercer ce droit de communication auprès des entreprises de transport terrestre, ferroviaire, maritime et aérien ainsi qu'auprès des agents et opérateurs de voyage et de séjour.

TRACFIN pourra ainsi obtenir des *« éléments d'identification des personnes ayant payé ou bénéficié d'une prestation ainsi que des éléments d'information relatifs à la nature de cette prestation et, s'il y a lieu, aux bagages et marchandises transportés »*. Cela lui permettra d'enrichir ses analyses et ses enquêtes en établissant *« une corrélation précise et étayée entre des flux financiers et des déplacements de personnes ou de marchandises »* selon les termes de l'étude d'impact du projet de loi.

*

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

*
* *

Après l'article 9

La commission examine l'amendement DN10 du rapporteur pour avis.

M. le rapporteur pour avis. Cet amendement vise à assurer une protection pénale aux agents des services de renseignement lorsqu'ils agissent hors du territoire national, sur le modèle de la protection offerte aux militaires déployés en opérations extérieures, dans le cadre de leur mission. Il reprend ainsi une des propositions formulées par la délégation parlementaire au renseignement dans son rapport d'activité 2014.

*La commission **adopte** l'amendement.*

*
* *

Article 10
(art. 323-8 *(nouveau)* du code pénal)
Protection pénale des agents des services de renseignement

Cet article vise à exonérer les agents des services de renseignement de poursuites pénales lorsqu'ils portent atteinte, pour les motifs d'intérêt public prévus par le nouvel article L. 811-3 du code de la sécurité intérieure, à des systèmes d'information situés hors du territoire national.

*

*La commission émet un avis **favorable** à l'adoption de l'article 10 **sans modification**.*

*
* *

Article 11
(art. 41 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
Contentieux de la classification des données protégées

Le présent article est relatif au contentieux de l'accès indirect à certains fichiers intéressant la sûreté de l'État. Il vise à préserver la confidentialité des informations contenues dans ces fichiers tout en garantissant les pouvoirs de contrôle du juge et les droits des requérants.

Ainsi, le juge obtiendra communication des éléments pertinents contenus dans ces fichiers, sauf à ce qu'ils soient couverts par le secret de la défense nationale. Ces éléments, bien que non versés au contradictoire, pourront fonder la décision du juge. S'il apparaît que le fichier ne comporte aucune mention erronée relative au requérant ou ne contient pas d'information à son sujet, la décision du juge ne pourra révéler s'il figure ou non dans le traitement ; inversement, le requérant pourra être informé par le juge si des informations le concernant sont irrégulièrement mentionnées dans le traitement.

*

*La commission émet un avis **favorable** à l'adoption de l'article 11 **sans modification**.*

*
* *

Article 12
(art. 39 de la loi n° 2009-1436 du 24 novembre 2009 pénitentiaire ; art. 727-2 et 727-3 *(nouveaux)* du code de procédure pénale)
Contrôle des communications électroniques des détenus par l'administration pénitentiaire

Le présent article vise à donner à l'administration pénitentiaire les moyens de procéder au brouillage des communications électroniques passées illégalement par les détenus, à intercepter leurs données de connexion et à exercer un contrôle sur les utilisations des ordinateurs portables.

Alors que 27 524 téléphones portables ou accessoires, introduits illégalement, ont été découverts par l'administration pénitentiaire en 2014 (contre 10 990 en 2010) et que 2 500 ordinateurs portables sont possédés, légalement, par les détenus, celle-ci ne dispose aujourd'hui pas des moyens nécessaires à un contrôle efficace des communications électroniques émises.

Le nouvel article 727-2 permettra à l'administration pénitentiaire de disposer des prérogatives nécessaires à la détection, au brouillage et à l'interruption des correspondances illicites émises ou reçues par la voie des communications électroniques ou radioélectriques par une personne détenue, c'est-à-dire notamment des communications téléphoniques, échanges de messages écrits ainsi que des communications par *talkie-walkie*.

Cet article autorise également l'administration pénitentiaire à utiliser des dispositifs techniques de proximité, c'est-à-dire des *IMSI-catchers*, pour recueillir les données de connexion ou celles relatives à la géolocalisation des équipements utilisés.

Le nouvel article 727-3 prévoit le cadre dans lequel les ordinateurs des personnes détenues peuvent être contrôlés, y compris en temps réel, pour détecter une éventuelle connexion illicite.

La mise en œuvre de ces deux dispositions sera placée sous le contrôle du procureur de la République.

*

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

*

* *

Article 13

(art. 6 *nonies* de l'ordonnance n° 58-11000 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires)

Dispositions transitoires, incompatibilité entre les qualités de membre de la CNCTR et de la délégation parlementaire au renseignement

Le présent article comporte des dispositions transitoires et prévoit que la CNCTR succède à la Commission nationale de contrôle des interceptions de sécurité.

Il dispose également que les membres de la délégation parlementaire au renseignement ne peuvent être nommés membres concomitamment de la CNCTR. Il s'agit là de distinguer le contrôle parlementaire – ou « *contrôle externe de responsabilité* » (1) – effectué par la délégation, du « *contrôle de légalité et de proportionnalité* » (2) effectué par la nouvelle Commission.

Si l'autorité indépendante s'assure que les demandes déposées par les services spécialisés respectent les conditions prévues par la loi, la délégation

(1) Expression utilisée dans le rapport d'information de la commission des Lois précité et le rapport d'activité 2014 de la délégation parlementaire au renseignement.

(2) Idem.

parlementaire au renseignement ne contrôle non pas les services mais leur utilisation par le pouvoir exécutif. Il s'agit donc bien de deux formes de contrôle, toutes deux indispensables à la garantie des droits, mais qu'on ne saurait associer. La présence des parlementaires au sein de la future commission doit être vue comme un moyen, par le pluralisme qu'elle devra respecter, de renforcer l'indépendance de cette institution, et non comme une quelconque volonté d'effectuer un contrôle de responsabilité.

*

La commission émet un avis ***favorable*** *à l'adoption de l'article 13* ***sans modification****.*

*

* *

Article 14

(art. L. 285-1, L. 286-1 et L. 287-1 du code de la sécurité intérieure, art. L. 2371-1 du code de la défense, art. L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense)

Coordination

Cet article de coordination procède aux abrogations rendues nécessaires par le projet de loi.

*

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

*

* *

Article 15

Coordination

Cet article étend l'application des articles 9 à 13 en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis-et-Futuna.

*

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

*

* *

Article 16
Coordination

Le présent article prévoit que, à l'exception des articles 9 à 12, la loi entre en vigueur à la date de publication au *Journal officiel* du décret nommant les membres de la CNCTR, dont la constitution est un préalable nécessaire à la mise en œuvre des techniques de renseignement prévues par la loi.

*

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

*Puis elle émet un avis **favorable** à l'adoption de l'ensemble du projet de loi **ainsi modifié.***

ANNEXES

ANNEXE 1

Auditions de la commission

Par ordre chronologique

1. Audition de M. le préfet Alain Zabulon, coordonnateur national du renseignement (mardi 17 mars 2015).

Mme la présidente Patricia Adam. Nous débutons aujourd'hui nos auditions sur la loi relative au renseignement, qui a été soumise au Conseil d'État et sera examinée jeudi en Conseil des ministres.

Monsieur le préfet, nous avons, dans ce cadre, souhaité vous inviter devant notre commission – où vous avez désormais l'habitude de venir régulièrement – afin que vous nous indiquiez quels sont les principaux objectifs pour vos services, les outils qui leur sont nécessaires, et que vous présentiez l'équilibre de ce texte.

M. le préfet Alain Zabulon, coordonnateur national du renseignement. La première raison d'un tel projet de loi, c'est que la France est l'une des dernières démocraties occidentales à ne pas disposer d'un cadre légal cohérent et complet régissant l'action des services de renseignement. C'est une situation préjudiciable à la fois aux services, parce qu'un certain nombre d'outils, n'étant pas prévus par la loi, ne leur sont pas accessibles, et aux libertés, l'absence de régime légal impliquant l'absence de contrôle.

Ce projet de loi s'inscrit dans la continuité d'un mouvement de réforme initié à partir de 2007. Cette année-là a été créée une délégation parlementaire au renseignement : pour la première fois était ainsi reconnu le contrôle du Parlement sur cette politique publique. En 2007 la notion de communauté du renseignement a été définie, autour de six services : la direction générale de la sécurité extérieure (DGSE), la direction générale de la sécurité intérieure (DGSI), la direction de la protection et de la sécurité de la défense (DPSD), la direction du renseignement militaire (DRM), la direction nationale du renseignement et des enquêtes douanières (DNRED), et le service Tracfin chargé du renseignement financier. A également été créé le Conseil national du renseignement, une instance présidée par le Président de la République et qui siège en présence du Premier ministre, des ministres ayant en charge les services de renseignement, des directeurs des services de renseignement dont la présence est requise, du coordonnateur national du renseignement, fonction elle-même créée en 2009 et du SGDSN qui en assure

le secrétariat. En 2010 a été créée une académie du renseignement chargée de former les cadres des services et en 2014 une inspection des services de renseignement, désormais opérationnelle.

Une autre raison de légiférer, est que nous avons été sensibles au fait que les révélations Snowden sur les activités de la NSA avaient pu susciter des interrogations et des inquiétudes dans l'opinion publique. Il était légitime d'apporter une réponse législative afin de montrer que la politique du renseignement telle qu'elle est conçue par le Gouvernement de notre pays ne relève pas de la même philosophie que celle qui prévaut aux États-Unis.

La volonté de légiférer a également été exprimée par le Parlement. Dans son rapport de mai 2013, intitulé *Pour un État secret au service de notre démocratie*, la mission d'information présidée par les députés Jean-Jacques Urvoas et Patrice Verchère a conclu à la nécessité d'une loi pour encadrer certaines activités des services.

Enfin, la loi du 10 juillet 1991 relative aux interceptions de sécurité – les fameuses écoutes téléphoniques, dont l'abus avait rendu nécessaire l'intervention du législateur – est antérieure à l'arrivée d'internet, du téléphone portable, de la massification des échanges d'informations sur les réseaux, et a donc considérablement vieilli.

Nous nous sommes mis au travail il y a plus d'un an. Ce projet de loi n'est ainsi nullement le résultat d'une réflexion précipitée à la suite des attentats de janvier, mais l'aboutissement d'une longue réflexion. Les attentats de janvier ont incité le Gouvernement à demander d'accélérer le calendrier et de tirer les enseignements de ces tragiques événements sur le plan opérationnel.

Ce texte répond à deux finalités. La première est de doter d'un cadre juridique les moyens techniques et opérationnels indispensables à l'accomplissement de leurs missions par les services de renseignement. En 1991, dans le cadre d'une écoute téléphonique, on écoutait une personne avec un téléphone filaire. Les individus que nous suivons aujourd'hui possèdent dix cartes SIM, cinq téléphones différents, une dizaine d'adresses internet, et utilisent des stratégies de contournement pour échapper à la vigilance des services.

Dans cette première partie du projet de loi, nous reprenons, en le toilettant, le dispositif des interceptions de sécurité et d'accès aux données de connexion tel qu'il résulte de la loi de 1991. Les données de connexion ne renseignent pas sur le contenu d'un échange ; elles indiquent par exemple que le portable de A s'est connecté au portable de B tel jour à telle heure. Elles peuvent apporter beaucoup d'informations sur la constitution de réseaux, les complicités entre individus, la préparation de projets. Dans le monde d'aujourd'hui, il est aussi important de savoir qui parle avec qui, que ce qui s'est dit. Le cadre juridique de l'accès à ces données a été défini par un article de la loi de programmation militaire de décembre 2013. La matière est reprise dans notre projet.

Ensuite, nous transposons dans le domaine de la prévention un certain nombre de techniques qui ne peuvent être utilisées actuellement que dans le cadre de procédures judiciaires. Dans ce cadre, en effet, les services de renseignement, sur instruction du juge, peuvent utiliser des techniques telles que le balisage de véhicules ou d'objets – pour en localiser les déplacements –, la sonorisation ou la captation d'images dans les lieux privés, la captation de données informatiques, et ils peuvent même procéder à des intrusions domiciliaires afin d'y installer ces moyens techniques. Le projet de loi a pour objectif de transposer l'ensemble de ces techniques dans le domaine de la police administrative, c'est-à-dire de la prévention. J'insiste sur la différence fondamentale, dans notre système juridique, entre la police administrative, qui vise à prévenir, et l'autorité judiciaire, dont l'objet est de réprimer. Le renseignement se situe très en amont du judiciaire et doit pouvoir intervenir sur certains individus à un moment où aucune infraction n'a été commise mais où il est indispensable de pouvoir lever le doute sur leurs intentions, avant, le cas échéant, de saisir l'autorité judiciaire s'il y a matière à le faire.

Nous estimons à plus de 3 000 le nombre d'individus qui, sur le territoire national, représentent, à des degrés d'intensité variable, une menace pour notre sécurité. Le grand défi des services de renseignement est de parvenir à détecter, parmi ces 3 000 individus, ceux qui sont susceptibles de passer à l'acte. Pour suivre physiquement un individu H24, il faut en moyenne dix-huit à vingt fonctionnaires de police, ce qui signifie que l'effectif de la DGSI devrait être de 60 000 fonctionnaires, contre les 3 200 qu'elle compte actuellement. Malgré les arbitrages du Gouvernement en vue d'augmenter les effectifs de ce service, ce serait entrer dans une logique folle que d'imaginer recruter en permanence des fonctionnaires pour courir après des terroristes. Pour être efficace, il faut donc pouvoir suivre en temps réel, sur internet et les réseaux, les connexions de ces individus, parce qu'elles nous renseignent sur leurs intentions. Savoir que tel individu s'est connecté à tel autre individu bien connu des services depuis des années est une information qui s'appelle un « signal faible », et le défi des services est d'être capable de détecter ces micro-informations qui, mises bout à bout, permettent de renseigner sur un éventuel projet d'attentat. Un article du projet de loi permettra donc d'accéder aux données de connexion des individus qui ont été repérés comme présentant une menace, de manière à suivre leurs intentions en temps réel.

Enfin, la loi fixe un cadre juridique pour les mesures de surveillance internationale. Ces mesures ne concernent que les personnes à l'étranger. La France est membre permanent du Conseil de sécurité de l'ONU ; elle est amenée à ce titre à prendre position sur les grands dossiers internationaux.

La DGSE, collecte du renseignement hors de nos frontières pour informer le gouvernement sur ces sujets. Nous avons souhaité fixer un cadre juridique car ces mesures d'interception – puisque c'est de cela qu'il s'agit –, couvertes par le secret de la défense nationale, sont parfois réalisées à partir du territoire national. Toutefois, le choix a été fait de réserver le régime juridique le plus protecteur pour

les actions sur le territoire national. L'utilisation de ces techniques intrusives est assortie d'un cadre juridique contraignant qui veille à garantir le respect des libertés de nos concitoyens : c'est la seconde partie du projet de loi.

Premier élément de garantie, la loi définit de manière limitative les finalités pouvant justifier l'utilisation de ces techniques. Les services de renseignement peuvent être autorisés à recourir à ces techniques « *pour le recueil de renseignements relatifs aux intérêts publics* » énumérés sous le chef de sept items correspondant aux actuelles missions des services. Un œil non averti pourrait s'imaginer que nous ouvrons un champ d'investigation illimité aux services de renseignement ; il n'en est rien, les finalités sont celles qui correspondent à l'action des services aujourd'hui.

Ces finalités sont la sécurité nationale, un concept reconnu en droit public, qui recouvre notamment la lutte contre la prolifération des armes de destruction massive, la contre-ingérence et le contre-espionnage : les intérêts essentiels de la politique étrangère ; les intérêts économiques et scientifiques essentiels de la France – cela vise les actions d'ingérence, en très forte augmentation, contre nos laboratoires et nos entreprises pour piller les technologies, nos savoir-faire, la recherche fondamentale, les nanotechnologies, l'aéronautique, le médical… – ; la prévention du terrorisme ; la prévention de la criminalité et de la délinquance organisées ; enfin, la prévention des violences collectives de nature à porter gravement atteinte à la paix publique – il ne s'agit en aucun cas d'utiliser les moyens du renseignement pour espionner des mouvements sociaux qui font partie de la vie politique de notre pays, mais de renseigner sur certains groupements qui pratiquent la violence de manière délibérée. Ces finalités, qui correspondent à celles qui sont déjà assignées aux services, chacun dans le cadre de leurs missions respectives, sont désormais inscrites dans la loi ; le progrès tient à un encadrement, qui faisait défaut jusqu'alors, de leur action

La procédure d'utilisation de ces techniques est très précisément définie. La demande doit être écrite et motivée. Elle est validée par le ministre en charge du service ou son directeur de cabinet. Les décisions d'autorisation sont prises par le Premier ministre, après l'avis d'une autorité administrative indépendante dont je parlerai tout de suite après. Ces décisions d'autorisation ont une durée maximale fixée par la loi : plus le moyen est intrusif et susceptible d'être attentatoire à la vie privée, plus la durée d'autorisation est encadrée. Elle ne peut être reconduite que selon les mêmes modalités que la demande initiale.

La clé de voûte du dispositif est l'intervention d'une nouvelle autorité administrative indépendante se substituant à la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Aux termes de la loi de 1991, cette dernière est censée émettre une simple recommandation *a posteriori*. La nouvelle loi met le droit en conformité avec la pratique, car cette commission émet dans la pratique des avis préalables. La Commission nationale de contrôle des techniques de renseignement (CNCTR) formulera un avis avant la décision du Premier ministre, et pourra contrôler l'utilisation des techniques et intervenir *a posteriori*.

Cette Commission serait composée de quatre magistrats ou anciens magistrats, d'une personnalité qualifiée pour sa connaissance en matière de communications électroniques, proposée par l'Autorité de régulation des communications électroniques et des postes (ARCEP) – il est important qu'un membre de cette Commission parle le même langage que les techniciens des services qui utilisent ces moyens très sophistiqués –, et de quatre parlementaires, deux députés et deux sénateurs, issus de la majorité et de l'opposition, de manière à renforcer l'indépendance de cette autorité.

Des garanties supplémentaires ont été prévues pour les techniques nécessitant une intrusion dans les lieux privés. Lors d'une perquisition judiciaire, les policiers, sous le contrôle du juge, peuvent ouvrir les tiroirs, fouiller, emporter les ordinateurs et les documents présents, tandis que l'intrusion domiciliaire n'est autorisée en police administrative que pour déposer un dispositif technique permettant de capter du son, de l'image ou des données informatiques. Une demande spécifique devra être formulée et les agents spécialement habilités. L'avis de la Commission devra avoir été rendu de manière expresse par l'un des quatre magistrats membres de la Commission.

Les durées maximales de conservation des données recueillies grâce à ces techniques sont également prévues par la loi.

Enfin, un droit au recours juridictionnel a été ouvert. Cela peut paraître banal mais, dans le domaine du renseignement, c'est une novation très importante. Le Conseil d'État pourra être saisi d'un recours juridictionnel par tout citoyen ayant intérêt à agir – toute personne estimant, à tort ou à raison, avoir fait l'objet d'une surveillance par l'une des techniques de renseignement que j'ai évoquées – après avoir déposé une réclamation auprès de la CNCTR. Le Conseil d'État pourra également être saisi par la CNCTR lorsque celle-ci estimera qu'une décision d'autorisation a été prise par le Premier ministre en méconnaissance de la loi. S'il juge qu'une illégalité a été commise, le Conseil d'État pourra annuler l'autorisation accordée, ordonner la destruction des renseignements illégalement obtenus, indemniser le requérant et saisir en cas d'infraction le procureur de la République.

Encore une fois, c'est une révolution. Nous avons estimé que ce projet de loi ne serait pas crédible s'il se contentait de donner des moyens techniques renforcés aux services, sans prévoir de garanties. Dans le grand débat, que nous aimons bien en France, entre libertés et sécurité, nous avons introduit un troisième terme : les garanties. C'est ce qui rend possible une action des services plus efficace sans porter atteinte aux libertés.

M. Philippe Nauche. Vous n'avez pas évoqué la protection de l'identité des agents, point sur lequel il semblerait que le texte n'apporte pas de précision particulière. Par ailleurs, qu'en est-il des échanges entre les six services composant la communauté du renseignement et les autres services qui concourent au renseignement sans faire partie de cette communauté : renseignement

territorial, renseignement pénitentiaire, service d'anticipation de la gendarmerie nationale ? Ces derniers sont-ils concernés par les mesures du texte ?

M. le préfet Alain Zabulon. Vous avez raison de souligner l'importance de coopérer avec les services hors de la communauté du renseignement. Cela se pratique très largement. En matière de lutte antiterroriste, par exemple, le nombre d'individus suspects est tel qu'une partie est suivie par la DGSI et l'autre par le service du renseignement territorial, sans parler de ceux qui le sont par la direction du renseignement de la préfecture de police de Paris. La DGSI a également des liens avec le renseignement pénitentiaire car le milieu carcéral, on le sait, est souvent un lieu de radicalisation. Nous n'avons pas attendu l'évolution officielle du périmètre de la communauté pour créer entre ces services les indispensables synergies sans lesquelles nous ne serions pas efficaces.

La loi traite indirectement de ces services en permettant qu'un décret en Conseil d'État puisse élargir de manière contrôlée l'utilisation de ces techniques par d'autres services hors de la communauté du renseignement. Ce décret précisera quels services, pour quelles missions et quelles techniques. Nous ne sommes pas favorables à ce que la loi permette l'utilisation sans contrôle, de toutes les techniques par tous les services. Nous voulons que cette extension soit maîtrisée, et ne serve pas pour toutes les finalités. Le renseignement territorial renseigne les préfets sur l'actualité économique et sociale du département ; il est hors de question d'utiliser des techniques intrusives pour renseigner sur des événements qui n'ont aucun rapport avec la sécurité nationale ou la prévention du terrorisme. En revanche, que le Service central du renseignement territorial (SCRT) demande l'utilisation de ces techniques pour suivre les quelques centaines d'individus qu'il surveille au titre de la prévention du terrorisme peut être pertinent.

Mme Agnès Deletang, magistrate, conseillère auprès du Conseil national du renseignement. La loi LOPPSI 2 de mars 2011 comportait trois types de dispositions protectrices des agents et des sources.

Tout d'abord, cette loi a inséré dans le code de la défense la légalisation de l'identité d'emprunt ou de la fausse qualité prise par un agent de renseignement dans le cadre d'une mission intéressant la défense et la sécurité nationale. L'article renvoie à un arrêté du Premier ministre qui liste les services pouvant prendre de telles dispositions pour leurs agents, et qui sont les six services de la communauté du renseignement.

De même, un article sanctionnant la révélation directe ou indirecte de toute information qui conduirait à divulguer l'appartenance d'un agent à un service de renseignement, le nom ou l'identité d'emprunt d'un agent ou d'une source d'un service de renseignement a été introduit dans le code pénal. Enfin, un article protégeant l'anonymat des agents des services spécialisés de renseignement appelés à témoigner lors de procédures judiciaires, afin que leur couverture ne soit pas dévoilée, a été inséré dans le code de procédure pénale. Il a été renforcé par la

loi de programmation militaire de 2013 : ce témoignage peut désormais s'effectuer dans un lieu que le directeur du service de renseignement peut choisir lui-même.

Il avait été envisagé de faire référence à ces articles dans le code de la sécurité intérieure, dans lequel s'insèreront les nouvelles dispositions ; si cela n'a finalement pas été estimé nécessaire, il a cependant été ajouté un nouvel article protecteur de l'anonymat des agents des services de renseignement, aménageant la publicité des actes réglementaires et individuels les concernant.

M. Sylvain Berrios. Ma question rejoint celle de M. Nauche, concernant la coordination des activités entre les services à l'intérieur de la communauté du renseignement et hors de cette communauté. Vous avez expliqué que cette loi fixait des finalités correspondant aux actuelles missions des six services de la communauté du renseignement. Or les services hors communauté du renseignement sortent de ce spectre et peuvent avoir leurs propres finalités. Je ne vois donc pas comment un décret en Conseil d'État pourrait coller parfaitement aux missions des six services.

M. le préfet Alain Zabulon. Si nous avons pris la peine d'inscrire les finalités dans la loi, ce n'est pas pour que d'autres services, qui font du renseignement tout en étant hors de la communauté, puissent s'en affranchir. L'article de la loi sur les finalités s'imposera si tel ou tel service hors communauté, tel que le renseignement territorial, venait à utiliser des techniques intrusives. Je prends l'exemple du renseignement territorial à dessein car c'est le service hors communauté dont le spectre d'activité est le plus large. Il fait du renseignement ouvert : il prend contact avec les acteurs institutionnels du département et rend compte au préfet. Il est tout à fait exclu de recourir à des techniques intrusives pour ce type de renseignement.

M. Jean-Jacques Candelier. Avez-vous, ces dernières années, été confrontés à des suppressions de postes ou baisses budgétaires ? De quels moyens supplémentaires disposez-vous depuis la mise en place du dispositif Sentinelle ? Sont-ils suffisants ? Enfin, il y aurait 3 000 personnes à risque dans notre pays ; sur quelle période est-on arrivé à ce chiffre inquiétant ?

M. le préfet Alain Zabulon. Nous sommes arrivés à ce chiffre en moins de deux ans. Sur ces 3 000 individus, il y a tout d'abord ceux qui sont impliqués dans les filières syro-irakiennes, au nombre de 1 432, un nombre qui se décompose comme suit : 413 individus détectés comme étant physiquement présents sur les théâtres de combat en Syrie, 295 en transit, c'est-à-dire en train de s'y rendre – nous invitons les autorités turques à les interpeller et à les renvoyer en France, –, 261 ayant quitté les zones de combat, dont 201 sont revenus en France, 85 présumés morts et 376 projetant de partir.

S'y ajoutent des individus radicalisés qui ne sont pas impliqués dans les filières mais présentent un profil suffisamment inquiétant pour représenter une menace, au nombre de 430. Le service de renseignement territorial suit les

individus réputés les moins dangereux, ceux dont on pense qu'ils sont davantage dans le verbe que dans l'action, au nombre d'environ 180. Si l'on y ajoute un millier de profils préoccupants d'individus détectés comme fréquentant assidûment les sites internet les plus radicaux, les sites terroristes, cela fait environ 3 000 personnes.

Tout cela est apparu dans des délais extrêmement brefs. Depuis trois ans, je rencontre régulièrement le directeur général de la sécurité intérieure ; nous ne parlons de ce phénomène des filières syriennes que depuis fin 2013, début 2014. Le nombre de 1 432 individus que j'ai cité représente une augmentation de 158 % en un an. Une explosion qui a incité le Gouvernement à agir dès le mois de mars 2014, avec une série de mesures arrêtées en Conseil de défense – création d'une plateforme téléphonique dotée d'un numéro vert, confiscation du passeport, instauration d'une procédure d'opposition parentale à la sortie du territoire de leur enfant mineur –, puis la loi antiterroriste de novembre, avant l'adoption de la loi sur le renseignement. La réponse étatique s'est construite étape après étape, à mesure que le phénomène grandissait.

Depuis les attentats, le Gouvernement a annoncé des arbitrages importants en faveur des moyens des services. Des mesures exceptionnelles ont été adoptées en Conseil des ministres le 21 janvier : création de 1 400 emplois sur trois ans au ministère de l'Intérieur, dont 1 100 pour renforcer le renseignement, et 530 dès cette année, création de 950 emplois au ministère de la Justice, de 250 emplois au ministère de la Défense, plus quatre-vingts emplois au ministère des Finances, dont une dizaine pour TRACFIN et soixante-dix pour les douanes, la direction du renseignement douanier jouant un rôle important dans la lutte contre cette menace terroriste. Cela représente environ 736 millions d'euros sur les trois prochaines années, dont 246 millions dès 2015.

Au moment où la DCRI est devenue la DGSI, en 2014, 432 recrutements étaient déjà prévus sur trois ans, ce qui signifie que, sur les trois années à venir, les effectifs de la DGSI grossiront d'environ un millier d'agents. C'est un effort substantiel.

En ce qui concerne le dispositif Sentinelle, le plan Vigipirate, permet de mobiliser 10 000 soldats pendant un mois. Nous avons largement dépassé la période d'un mois. C'est un effort très important : 10 000 soldats, c'est près de trois fois les effectifs de l'opération Barkhane dans la bande saharo-sahélienne. Le Président de la République a décidé de sanctuariser le budget du ministère de la Défense, qui restera à 31,4 milliards d'euros ; ces dépenses seront couvertes par redéploiements.

Les services de renseignement ont vu leurs effectifs préservés et même, pour certains d'entre eux, augmenter, ce qui correspond à la nécessité à laquelle nous sommes confrontés.

M. Joaquim Pueyo. Le fait d'accorder un accès administratif plus grand aux services de renseignement est nécessaire, mais c'est tout de même un changement de culture, car on fait sortir le magistrat du dispositif. Pour compenser cela, la loi crée la CNCTR, où siégeront des magistrats et anciens magistrats. Nous sommes un État de droit et il convient de prévoir des contrôles fins garantissant le respect des libertés individuelles. Qui désignera les membres de cette nouvelle Commission ?

M. le préfet Alain Zabulon. Vous avez raison de souligner que le mode de désignation de ses membres joue un rôle important dans la crédibilité de cette commission. Les deux députés et sénateurs seront, je cite l'article, « *désignés respectivement, pour la durée de la législature, par le président de l'Assemblée nationale et, après chaque renouvellement partiel du Sénat, par le président du Sénat, de manière à assurer une représentation pluraliste du Parlement* ». Siégeront par ailleurs deux membres ou anciens membres du Conseil d'État d'un grade au moins égal à celui de conseiller d'État, nommés sur proposition du vice-président du Conseil d'État. Cela signifie que sera pris un décret recognitif dans lequel ne pourront être retenus que les deux noms proposés. Il en va de même pour la Cour de cassation, avec une proposition conjointe du premier président et du procureur général. Enfin, la personnalité qualifiée sera nommée sur proposition du président de l'ARCEP. Sur l'ensemble des membres, l'exécutif n'intervient pas puisque ce sont les institutions d'origine qui les désignent.

En revanche, nous sommes attachés à ce que le Gouvernement conserve le pouvoir de désignation du président de l'instance, qui devra obligatoirement être choisi parmi les magistrats ou anciens magistrats. Cette désignation par l'exécutif ne sera pas un cas unique parmi nos autorités indépendantes. Dans un domaine éminemment régalien, il n'est pas illégitime que le Gouvernement choisisse le président de la commission de contrôle, sans que cette formule n'altère en quoi que ce soit son indépendance. C'est déjà le cas avec le président de l'actuelle CNCIS dont l'indépendance n'est contestée par personne.

M. Joaquim Pueyo. Le fait que le président soit nommé parmi les magistrats est un point important. Quant au choix de deux députés, le texte précise-t-il que l'un doit être de la majorité et l'autre de l'opposition ?

M. le préfet Alain Zabulon. C'est un peu plus souple que cela : le texte prévoit « *une représentation pluraliste du Parlement* », comme c'est le cas pour l'actuelle CNCIS.

M. Joaquim Pueyo. Il faut être très précis. J'y insiste, car j'ai quelques inquiétudes pour l'avenir.

M. le préfet Alain Zabulon. Quand vous dites que le juge est absent du dispositif, je ne partage pas votre point de vue. C'est vrai pour le juge judiciaire mais non pour le juge administratif. Le Conseil d'État jouera un rôle de recours juridictionnel de plein exercice. Comme en témoigne sa jurisprudence, le juge

administratif est aussi exigeant que le juge judiciaire en matière de protection des libertés.

M. Joaquim Pueyo. Ce n'est pas la même chose, et il est d'ailleurs bon que le premier président et le procureur général de la Cour de cassation désignent des magistrats de l'ordre judiciaire. Le juge judiciaire ne doit pas être écarté.

M. le préfet Alain Zabulon. Nous partons de rien. Les interceptions de sécurité conduites par les services de renseignement ne font aujourd'hui intervenir aucun juge. La CNCIS, si elle estime qu'une technique a été indûment utilisée, peut faire une recommandation *a posteriori*. Enfin, quand un administré présente une réclamation, on lui répond : « Nous avons vérifié : tout va bien. » Je ne caricature pas. L'état du droit, actuellement, c'est à peu près le néant.

Nous avons construit un dispositif global dans lequel les garanties sont aussi consistantes que les moyens accordés aux services. Nous avons eu de très longues séances au Conseil d'État, chaque article a fait l'objet d'une analyse très approfondie : le Conseil d'État nous a donné quitus de ce que ce texte réalisait un équilibre satisfaisant entre les deux exigences. Il a notamment démontré qu'une politique de prévention pouvait se placer sous l'empire de la police administrative sans que le droit ne s'en trouve violé. Son avis sera rendu public jeudi, en même temps que le projet de loi.

M. Daniel Boisserie. En écoutant votre réponse à Philippe Nauche, j'ai cru comprendre que la DGSI avait la compétence du renseignement en milieu carcéral.

M. le préfet Alain Zabulon. Le renseignement en milieu carcéral est traité par un service *ad hoc*, le service du renseignement pénitentiaire, qui relève de la direction de l'administration pénitentiaire, et dont les moyens ont été renforcés à la faveur des arbitrages postérieurs aux attentats de janvier.

La radicalisation en milieu carcéral est un vrai sujet. Un certain nombre d'individus entrent petits délinquants et sortent djihadistes, car ils ont été en contact avec des individus fanatisés et radicalisés qui leur ont « lavé le cerveau » en quelques semaines. D'où l'expérimentation, qui est en voie d'extension, consistant à isoler les détenus déjà radicalisés pour éviter qu'ils ne contaminent les autres. Il ressort en première analyse que le climat en détention s'est apaisé à la suite de cette mesure, car les moyens de pression parfois violents utilisés par les détenus radicalisés créent un climat de tension extrême.

Le nombre de personnes détenues, prévenues ou condamnées pour faits de terrorisme est de 170 ou 180. Le lien avec la DGSI est essentiel au moment où ces individus sortent de prison. Il faut absolument que ce service continue de les suivre. Cette synergie entre les deux services existe, un protocole a été signé. Le DGSI me fait part du climat tout à fait constructif dans lequel se passe cette collaboration.

M. Daniel Boisserie. Vous avez évoqué 3 000 individus, une courbe de croissance vertigineuse. Quel est votre pronostic pour l'avenir ? Par ailleurs, où en est l'Europe en ce qui concerne le projet de fichier PNR (*Passager Name Record*) ?

M. le préfet Alain Zabulon. Le PNR français a été voté dans la loi de programmation militaire, les décrets d'application sont parus, et il devrait entrer en application progressivement d'ici fin 2015, début 2016, nécessitant l'intégration des données de plus de 230 compagnies aériennes et plates-formes de réservation. Il permettra de collecter les données de réservation des passagers entre la France et l'étranger, hors Union européenne, c'est-à-dire que nous pourrons suivre le passager d'un vol Paris-Berlin mais non celui du vol Berlin-Rome : il aurait fallu, pour cela, que l'Allemagne et l'Italie aient chacune leur propre PNR. Le PNR français ne verra ainsi qu'une partie de l'information. Des démarches ont donc été entreprises par le ministre de l'Intérieur auprès des autorités européennes pour que l'Europe se dote de cet outil absolument indispensable. Cela suscite un débat sur la protection des données, mais une personne qui réserve un billet d'avion ne dévoile pas ses opinions politiques, sa religion ou ses orientations personnelles. Ces données de réservation peuvent être utiles aux services de renseignement car elles permettent de connaître les trajets des individus qui les intéressent.

Le PNR européen avance laborieusement. Il existe encore un blocage au niveau de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen. Nous espérons que le sujet évoluera positivement dans les mois à venir et le ministre de l'Intérieur s'est fortement mobilisé sur le sujet. Nous avons quelques alliés, notamment les Britanniques, qui ont déjà leur propre PNR eux aussi. Les Allemands sont plus partagés.

S'agissant de votre seconde question, nous ne sommes pas optimistes pour l'avenir. Nous pensons que ce phénomène de djihad à la française est désormais durablement ancré dans une partie de notre jeunesse. Je préfère parler d'idéologie plutôt que de religion, car ces jeunes gens ont en réalité une formation religieuse des plus sommaires, voire inexistante. Ils voient dans le djihad un exutoire à leurs frustrations. Ces jeunes gens se marginalisent en basculant dans la radicalité. Ils y trouvent un nouveau sens à leur vie. J'appelle d'ailleurs votre attention sur l'effet d'attractivité extrêmement puissant exercé par le mouvement Daech sur cette fraction heureusement très minoritaire de notre jeunesse.

Le phénomène n'est pas uniquement français. La Belgique est au moins aussi touchée que la France, comme nous l'avons vu avec les récentes interpellations de Verviers. Des pays comme le Canada ou l'Australie sont également concernés. Cela relativise les explications franco-françaises qui consistent à dire que tout cela serait le résultat de l'échec de nos politiques d'intégration, politiques de logement, politiques de la ville. Que ces politiques aient été insuffisantes pour réaliser l'intégration, c'est vrai, mais cette explication n'est pas suffisante. Le phénomène du djihad est aujourd'hui mondial. Dans les

troupes de Daech, les contingents les plus importants sont ceux des pays du Maghreb, comme la Tunisie. Si quelque 400 Français sont sur place, les Tunisiens sont plus de 3 000.

La poussée de l'islamisme radical et l'émergence d'un mouvement terroriste qui s'est transformé en État, ont tellement bouleversé cette partie du monde que l'influence du phénomène sur une fraction de notre jeunesse est, je crois, durable. La réponse de l'État ne peut être uniquement sécuritaire ; elle doit être également sociétale, par l'éducation, par la représentation du culte musulman en France, par un contre-discours déconstruisant le processus de radicalisation. Le phénomène est nouveau et le contre-discours reste encore à bâtir.

M. Jean-Michel Villaumé. Nos services de renseignement ont pointé, il y a quelques mois, le manque de coopération avec nos partenaires étrangers. Comment serait-il possible d'améliorer la synergie internationale, notamment concernant la question des combattants étrangers en Syrie, dont 90 % se recrutent par internet ? Les moyens sont-ils suffisants pour permettre de développer cette synergie essentielle ?

M. Alain Zabulon. La coopération avec nos partenaires étrangers est intense. Nous travaillons en très bonne intelligence – c'est le cas de le dire – avec nos homologues britanniques et américains. Ce sont ceux avec qui la coopération en matière de lutte contre le terrorisme est la plus ancienne et la plus forte. Nous coopérons de plus en plus avec l'Allemagne mais aussi avec d'autres pays européens

On pense parfois que cette coopération est inexistante parce qu'elle reste secrète. Elle doit le rester. Nous ne pouvons mettre sur la place publique tout ce que nous faisons en matière de coopération, qui, je vous rassure, n'attente en rien aux libertés, mais passe par le maniement d'informations très sensibles. Il existe une règle fondamentale dans les relations entre services de renseignement, la règle du tiers service : si je vous donne une information, vous ne devez jamais la révéler à un tiers sans mon autorisation. Cette relation reste donc très discrète mais elle est néanmoins tout à fait efficace.

Certains voudraient que nous allions vers l'Europe du renseignement. L'Europe peut apporter une aide sur certains points : il existe déjà des structures qui produisent de la synthèse, de l'analyse, de la coordination stratégique. Mais il ne peut y avoir d'Europe opérationnelle du renseignement. Les traités de l'Union donnent aux États une compétence exclusive en la matière.

J'ai des relations très suivies avec mes homologues, par exemple le DNI (*Director of National Intelligence*) américain, le patron des seize agences de renseignement, avec lequel j'ai tous les mois une visioconférence, ou que je rencontre, à Paris ou à Washington. Nous échangeons sur nos pratiques et nos analyses stratégiques.

Autant en matière économique, nous n'avons pas d'amis, seulement des concurrents –, autant en matière de contre-terrorisme, c'est l'union sacrée, car nous savons que tous nos pays peuvent être frappés.

M. Philippe Vitel. Vous avez évoqué les centaines de Français qui partent pour la Syrie et l'Irak. Quelles informations avez-vous sur d'éventuels départs de Français en Afrique pour rejoindre Boko Haram ? Ce dernier groupe venant de faire allégeance à l'État islamique, n'est-ce pas là une source de problèmes à venir, dans la mesure où nous avons en France, dans nos quartiers, beaucoup de jeunes musulmans d'origine africaine ?

Ensuite, la loi va faire peser de nouvelles contraintes sur les opérateurs de réseaux sociaux. Y sont-ils préparés ? Comment fonctionnera l'interaction de vos services avec ces opérateurs ?

Enfin, s'agissant de la cybersécurité, quelles sont vos relations avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ?

M. le préfet Alain Zabulon. Par sa nature et son intensité, le phénomène des filières syriennes est inédit. Nous avions perçu certains signes annonciateurs. Quand la France était présente en Afghanistan, quelques combattants français, de l'ordre d'une vingtaine, étaient partis dans ce pays. Lorsque l'opération Serval s'est déclenchée au Mali, les velléités de départ ont été vite contrariées, l'armée française ayant obtenu des résultats très rapides sur le terrain, et il ne s'est pas créé de filière malienne. À notre connaissance, il ne se crée pas non plus de filière vers Boko Haram, et la déclaration d'allégeance de ce mouvement à Daech, ne nous fait pas craindre, à court terme, compte tenu des distances entre les théâtres d'opérations et des capacités d'organisation logistique de ces groupes, un phénomène de coagulation qui verrait se créer une immense armée terroriste.

Boko Haram a un agenda régional. Son objectif est de créer le califat au nord du Nigéria, dans la région des grands lacs. D'autres mouvements, comme Al-Qaïda, ont un agenda international. Al-Qaïda maintient l'objectif de frapper ce qu'il appelle l'ennemi lointain. Aujourd'hui, Al-Qaïda dans la péninsule arabique est le mouvement terroriste le plus à même de projeter un attentat en Europe. Ce qui rassemble ces mouvements, c'est la haine de l'Occident. Le premier pays visé – cela figure dans les déclarations de tous leurs leaders du terrorisme international –, c'est la France, car notre pays est engagé militairement dans le combat contre le terrorisme, il participe aux frappes en Irak pour contrer les menées territoriales de Daech, il est engagé au Sahel, et par ailleurs, en matière de politique intérieure, notre concept de la laïcité, notre loi sur le voile, les débats sociétaux sur la place de l'islam, sont perçus ou interprétés par ces mouvements comme des agressions contre le monde musulman.

Pour le moment, le phénomène des combattants étrangers se limite à la Syrie. Nous ne voyons pas de filière se créer vers Boko Haram, et je ne crois pas vraiment à une telle éventualité.

En ce qui concerne les opérateurs, Mme Deletang était présente ce matin à une réunion que nous avons organisée pour leur présenter le texte de loi, qui leur créera certaines obligations. Ils ne sont pas inquiets, dès lors qu'ils auront une base légale. Ils souhaitent par ailleurs qu'il n'y ait pas de distorsion de concurrence, comme ce serait le cas si les obligations étaient imposées à certains et non à d'autres.

Mme Agnès Deletang. Des discussions auront lieu dans les semaines à venir avec les opérateurs. Ils considèrent que, compte tenu de l'évolution des technologies, le champ de la loi devrait concerner l'ensemble d'entre eux. Ils indiquent travailler en confiance avec le groupement interministériel de contrôle (GIC), le service spécialisé du Premier ministre centralisant les interceptions de sécurité du régime de la loi de 1991.

M. le préfet Alain Zabulon. Nous constatons une augmentation très forte des attaques cyber et un degré de sophistication toujours plus poussé. L'ANSSI, qui n'est pas un service de renseignement, a bénéficié dans la période récente d'arbitrages favorables : ses effectifs sont en augmentation et ses moyens juridiques ont été accrus par la loi de programmation militaire de décembre 2013. Devenue l'autorité d'État dans le domaine cyber, elle a créé une obligation de déclaration auprès d'elle des attaques cyber constatées par les opérateurs d'importance vitale. Sa mission est de protéger les sites informatiques de nos grandes administrations et institutions, à l'aide d'un système de veille H24 très performant.

Les services de renseignement ont évidemment leur rôle à jouer dans la détection des attaques. Nous développons nos propres moyens de cyber-attaques, dans une logique non pas agressive mais de dissuasion. S'il y a un domaine dans lequel il ne faut pas prendre de retard, c'est bien celui-là. Tous les conflits mondiaux montrent que l'arme cyber, non létale, anonyme, est très largement utilisée. On le constate dans tous les conflits internationaux en cours.

M. Gwendal Rouillard. Comment qualifiez-vous la capacité de nos services à travailler entre eux, à la fois sur notre sol et sur les théâtres extérieurs ? Je pense en particulier à la cellule Hermès, que le ministre de la Défense a évoquée ici. Par ailleurs, pouvez-vous préciser notre politique de renseignement concernant les individus radicalisés de retour d'Irak et de Syrie ? C'est un sujet qui donne lieu à débat.

M. le préfet Alain Zabulon. La culture traditionnelle de la communauté du renseignement privilégie la coopération bilatérale. Il existe par exemple ainsi un axe fort DGSE-DGSI – les relations entre les deux n'ont jamais été aussi intenses –, un axe fort DGSE-DRM, les deux ayant vocation à faire du renseignement à l'extérieur du territoire national, un axe fort DNRED-DGSE, la DNRED, qui lutte contre les grands trafics internationaux, ayant des méthodes d'action de terrain proches de celles de la DGSE. Je pourrais ainsi multiplier les exemples.

Un mois après les attentats de janvier, une fois passée la période d'émotion et de pression très forte sur les services, j'ai organisé une réunion sur les enseignements à tirer de ces attentats. Le consensus s'est dégagé autour de l'idée qu'il fallait intensifier la coopération multilatérale qui se développe déjà rapidement. La DGSI accueille dans ses locaux, à Levallois, des officiers de liaison des autres services qui viendront échanger sur les individus qu'ils suivent avec les services partenaires. Sur un même individu, la DNRED pourra par exemple, s'adresse à Tracfin pour connaître les mouvements sur sa carte bleue, à la DPSD s'il s'agit d'un ancien militaire radicalisé… Tous ces éléments convergent vers la DGSI qui est le chef de file en matière de lutte antiterroriste sur le territoire national.

La cellule Hermès l'avait un peu préfigurée. C'est, dans les locaux de l'état-major des armées, un espace ouvert aux six services de renseignement qui viennent tous les jours échanger sur les filières syriennes. C'est un lieu de synthèse du renseignement, qui reçoit un soutien appuyé du ministre de la Défense, véritable préfiguration de la communauté du renseignement de demain fondée sur la coopération multilatérale. Le grand défi des services, je l'ai dit, est la capacité de détecter des signaux faibles. Un individu souscrivant un emprunt à la consommation, et qui en retire le montant en liquide le lendemain peut être une information stratégique si elle est bien exploitée.

S'agissant des individus radicalisés de retour des théâtres de combat, ils font presque systématiquement, quand ils sont détectés, l'objet d'une interpellation par la DGSI.

Lorsqu'il y a matière à saisir le parquet antiterroriste, la DGSI le fait immédiatement, tandis que les autres continuent de faire l'objet d'un suivi attentif de la part des services.

Je souligne que le fait que notre pays soit doté d'un parquet antiterroriste, qui travaille en bonne intelligence avec les services de renseignement, est un atout qui nous est envié par d'autres pays.

2. Audition de M. Bernard Bajolet, directeur général de la sécurité extérieure (mardi 24 mars 2015).

Mme la présidente Patricia Adam. Notre commission conduira cette semaine plusieurs auditions sur le projet de loi relatif au renseignement qui sera discuté dans l'hémicycle à partir du lundi 13 avril, pendant environ une semaine. Nous sommes saisis pour avis, la commission au fond étant la commission des Lois, et nous nommerons notre rapporteur pour avis à la suite de cette audition.

Nous recevons aujourd'hui M. Bernard Bajolet, directeur général de la sécurité extérieure. Le texte sur le renseignement n'est pas une conséquence des événements de janvier, car il est en préparation depuis un an et demi. La question du renseignement avait fait l'objet d'un groupe de travail au sein de la commission du Livre blanc, et la réflexion s'est poursuivie dans les différents services, pour aboutir au texte qui nous est proposé.

M. Bernard Bajolet, directeur général de la sécurité extérieure. Ce projet de loi est un texte très important puisque c'est le premier texte de portée générale encadrant l'activité des services de renseignement depuis la Seconde Guerre mondiale. Il a une portée bien plus vaste que la loi de 1991, qui ne concernait que l'interception des communications. Ce projet de loi définit les missions des services de renseignement, les techniques qu'ils sont autorisés à employer sur le territoire national, ainsi que les modalités du contrôle de l'utilisation de ces techniques par une nouvelle commission, la Commission nationale de contrôle des techniques de renseignement (CNCTR).

La loi de 1991, si elle a été une excellente loi, a fait son temps, les techniques ayant énormément évolué depuis cette époque où n'existait que le téléphone fixe. Nous avons connu depuis lors l'explosion d'internet et du téléphone portable, et les individus auxquels nous nous intéressons disposent de multiples adresses électroniques, de plusieurs numéros de téléphone portable, et sont présents sur les réseaux sociaux.

La loi de 1991 prévoyait en outre une exception pour la DGSE, puisque les communications à l'étranger, qui sont notre cœur de métier, passaient essentiellement à l'époque par la voie du satellite, et que son article 20 exemptait du contrôle qu'elle instaurait les transmissions par liaison hertzienne.

C'est grâce à la jurisprudence, que l'on peut qualifier de créative, de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) que nous avons pu combler le fossé qui s'est progressivement élargi entre les dispositions légales et l'évolution des techniques. Nous travaillons sur la base de cette jurisprudence. C'est certes un cadre légal mais, dans le système français où la jurisprudence n'a pas la même force que dans les pays anglo-saxons, une telle base juridique est malgré tout assez fragile. Nous sentions bien la nécessité de

consolider ce cadre, surtout depuis l'affaire Snowden. Ce projet de loi est donc indispensable.

Bien que l'actualité dramatique du mois de janvier et les attentats plus récents commis au Mali, puis en Tunisie, montrent la réalité de la menace terroriste, la DGSE n'est pas chargée seulement de détecter ces menaces et de les prévenir. Elle a aussi pour mission d'informer les autorités politiques en matière de politique étrangère et de permettre au Gouvernement de disposer d'une capacité d'analyse autonome sur la situation de l'ensemble des pays du monde. La DGSE intervient également en soutien aux forces armées sur les théâtres d'opération. Nous avons en outre des missions de lutte contre la prolifération des armes de destruction massive, de lutte contre la criminalité internationale, ainsi que de soutien à notre économie et à nos entreprises. Les finalités définies dans le projet de loi, qui figureront à l'article 811-3, paraissent couvrir la gamme de nos missions.

L'article le plus important pour mon service est celui relatif à la surveillance internationale. Cet article L. 854-1 prend en considération la réalité des activités que nous menons. Sa rédaction nous convient. Cet article n'offre aucune capacité nouvelle par rapport à ce qui est aujourd'hui pratiqué et consacré par la jurisprudence de la CNCIS.

Il indique que les flux que nous interceptons portent sur les transmissions émises ou reçues à l'étranger. Le « ou » est important car cela signifie que ces communications peuvent être des communications mixtes, dont l'un des identifiants est rattaché au sol français. Dans ce cas, les conditions d'exploitation et de conservation des correspondances afférentes sont alors celles du droit commun, c'est-à-dire qu'elles sont exploitées dans un centre du GIC, service du Premier ministre, sous le contrôle de la CNCTR, sous réserve que leur délai de destruction court à compter de leur première exploitation.

Le texte renvoie à deux décrets, un décret en Conseil d'État pris après avis de la CNCTR, et un décret qui sera également soumis à la CNCTR mais non publié car nous ne souhaitons pas révéler publiquement certaines dispositions. Mais, ce deuxième décret sera, en plus, porté à la connaissance de la Délégation parlementaire du renseignement.

D'autres mesures du texte sont importantes. Je les aborderai sans doute en répondant à vos questions.

Mme la présidente Patricia Adam. Une question que nous avons longuement abordée dans le Livre blanc concerne la protection des agents, en particulier ceux de vos services. Estimez-vous que le texte répond à cette préoccupation ?

M. Bernard Bajolet. Le texte, à son article 10, prévoit une protection des agents mais pour des activités informatiques intrusives qu'ils mèneraient à partir du territoire français et visant des objectifs étrangers. La disposition est donc

limitée, et nous serions favorables à une mesure qui assurerait la protection pénale, dans leur propre pays, des agents pour l'ensemble des activités qu'ils mènent à l'extérieur de nos frontières, dès lors que celles-ci relèvent de leurs missions telles que définies par la loi. Cela rapprocherait le statut de mes agents de celui des militaires, protégés par une disposition du code de la défense.

M. Jean-Jacques Candelier. Malgré les révélations de l'affaire Snowden et la réforme promise par la Maison blanche, la NSA poursuivrait ses pratiques d'espionnage de masse en toute impunité. Qu'en pensez-vous ? Certains affirment que la NSA espionne la majorité des ordinateurs dans le monde ; que pensez-vous de la technologie qui permet de cacher des logiciels espions dans des disques durs ?

M. Bernard Bajolet. La NSA est tenue d'obéir à la loi américaine, comme la DGSE à la loi française, et il se trouve que la loi américaine n'interdit pas les activités en question. Cela ne signifie pas que nous les applaudissions, et c'est d'ailleurs pourquoi il est important de doter nos services de capacités qui leur permettent d'être indépendants des Américains. Si nous travaillons certes avec leurs services, l'un de nos objectifs, mis en lumière par l'affaire Snowden, est précisément de nous rendre moins dépendants d'eux et de renforcer la coopération avec nos partenaires européens.

Pour cela, il convient de doter nos services d'un instrument qui leur permettrait de détecter la préparation d'un attentat terroriste sur notre sol au moyen de l'exploitation de données techniques. C'est l'objet des articles 851-3 et 851-4, qui permettraient au GIC, de recueillir des métadonnées dans deux cas. Dans le premier cas, il s'agit de confronter ces métadonnées à des listes d'individus présentant une menace. Ces métadonnées restent anonymes jusqu'au moment où l'on détecte quelque chose qui conduit à demander une interception de sécurité.

Dans le second cas, il s'agit de détecter certaines pratiques de communication. L'objectif n'est pas de surveiller des comportements sociaux, tels que la fréquentation de telle ou telle mosquée par telle ou telle personne. Mais nous connaissons les techniques qu'emploient les djihadistes pour dissimuler leurs communications et échapper à toute surveillance : ce sont ces attitudes de clandestinité qu'il s'agit de détecter afin de prévenir des attentats, sans avoir à pratiquer une surveillance de masse.

M. Philippe Nauche. Quel avis portez-vous sur le contrôle de la CNCTR ? Quels sont, pour votre service, les avantages et les inconvénients d'un élargissement du domaine du contrôle ? Cela va-t-il contribuer à démystifier les choses ou bien cela peut-il constituer un frein à l'action de votre service ?

Les dispositions du texte concernent-elles bien seulement les personnes qui ayant la nationalité française ou domiciliées en France ?

Enfin, j'ai bien noté vos propos sur la protection des agents menant des actions à l'étranger. J'espère que la commission de la Défense y sera sensible et adoptera un amendement sur l'exemption de responsabilité, comme pour les militaires en opérations extérieures.

M. Bernard Bajolet. Dans la loi de 1991, il n'existe aucun contrôle sur les activités extérieures de mon service, puisqu'une exception a été prévue pour les transmissions par ondes hertziennes. La nouvelle loi instaure un régime de contrôle de la surveillance internationale calqué sur la jurisprudence qui s'est développée au gré de l'évolution des moyens de communication. L'équilibre trouvé entre les besoins des services et le contrôle nous paraît satisfaisant. Le contrôle par une autorité administrative indépendante légitime l'action des services et la sécurise, permettant d'établir une relation de confiance non seulement avec la CNCTR mais aussi avec la délégation parlementaire au renseignement. Notre souci, dans les discussions, était que ce contrôle légitime que nous appelons de nos vœux ne paralyse pas l'action des services. La disposition retenue concernant la surveillance internationale nous semble équilibrée.

La loi ne comporte pas à ce stade de distinction entre les étrangers de passage en France et les personnes de nationalité française ou résidant habituellement sur le territoire. La réflexion est cependant pertinente, dans la mesure où mon service est amené à suivre des objectifs étrangers lorsqu'ils se trouvent sur le sol national. Cela n'est pas explicitement pris en compte par la loi.

M. Eduardo Rihan Cypel. Ce texte, vingt-quatre ans après le précédent, était très attendu pour adapter les moyens juridiques et techniques des services de renseignement à l'évolution de la menace ainsi que des technologies de communication. Vous avez évoqué les différentes missions remplies par votre service, telles que la contre-prolifération nucléaire et l'analyse des enjeux de politique étrangère. Compte tenu de l'évolution de la menace terroriste, ce texte vous permettra-t-il de continuer à vous consacrer pleinement à ces autres missions, qui sont tout aussi importantes pour les intérêts de la France ?

M. Bernard Bajolet. Dans les débats internes que nous avons eus, j'ai beaucoup insisté sur le fait que, si notre service est appelé à détecter les menaces dans différents domaines – terrorisme, grande criminalité, espionnage –, il répond également à des enjeux géopolitiques et économiques. Les finalités énumérées dans le projet de loi recouvrent bien ces différentes activités.

Cette liste de finalités combine les cinq motifs figurant dans la loi de 1991 avec un autre motif qui figurait également dans cette dernière loi mais seulement à son article 20 : les « intérêts fondamentaux de la nation ». Si cette notion est déclinée à l'article 410-1 du code pénal, certains commentateurs ont jugé qu'elle n'était pas suffisamment précise. D'où l'idée de combiner certains aspects de cette notion, notamment les intérêts de la diplomatie et de la défense, avec les cinq motifs.

Cela ne devrait pas avoir d'incidence sur nos services, même si l'on peut s'interroger sur les qualificatifs qui nuancent cette énumération, tels que le terme « essentiel » dans les expressions « les intérêts économiques et scientifiques essentiels » ou encore « les intérêts essentiels de la politique étrangère ». Qui va décider de ce qui est essentiel ? Est-ce à une autorité administrative indépendante d'apprécier cela ?

Mme Patricia Adam. Surtout pas !

M. Bernard Bajolet. Vous avez raison de souligner, monsieur le député, que l'actuelle préoccupation pour la lutte contre le terrorisme ne doit pas nous faire perdre de vue nos autres missions. À la suite des attentats de janvier, les services, DGSI, DGSE, DPSD, ont reçu des moyens supplémentaires ; le Premier ministre a annoncé notamment la création de 185 emplois supplémentaires à la DGSE et soixante à la DPSD, dans le domaine de la lutte contre le terrorisme. Ces agents renforceront nos dispositifs aussi bien en matière technique que dans le renseignement humain. Pour autant, nous n'oublions pas nos autres priorités, notamment la géopolitique, parce qu'en la matière nous sommes bons sur certaines zones, certains pays, mais moins sur d'autres, ce qui exige encore des efforts de notre part. De la même façon, il ne faut pas oublier notre mission en matière économique, qui est essentielle.

M. Alain Moyne-Bressand. Comment s'organise la coopération internationale avec les autres organismes de renseignement, dans les pays confrontés comme nous à des problèmes de terrorisme ? Les renseignements sont-ils toujours donnés en toute transparence ?

M. Bernard Bajolet. Nous avons une coopération très étendue avec des partenaires étrangers. La DGSE en compte environ 200, services extérieurs mais aussi services intérieurs ou encore agences techniques, puisque, dans certains pays, comme les États-Unis ou l'Angleterre, ces agences sont séparées des autres services. Nous avons également des partenariats avec des pays que l'on pourrait par ailleurs considérer comme des adversaires. En matière de renseignement, tout le monde est un peu partenaire et adversaire à la fois. Certains sont plus partenaires qu'adversaires, et inversement.

Les partenariats sont particulièrement étendus en matière de terrorisme. Leur efficacité dépend de celle des services : ce n'est pas seulement une question de bonne volonté, cela dépend parfois aussi des capacités existantes. Cette coopération est sans réserve avec nos partenaires européens, dont certains possèdent des capacités remarquables. Elle est très bonne avec nos partenaires américains, comme avec les *Five Eyes* en général. Nous collaborons aussi avec les services russes, chinois et bien d'autres.

M. Daniel Boisserie. Quelles sont vos conclusions sur les attentats de Paris ? Avez-vous le sentiment que les moyens, financiers, techniques ou humains, étaient déficitaires ? Y a-t-il eu des dysfonctionnements administratifs ?

Reste-t-il encore une place pour le renseignement économique ? Par les temps qui courent, vous êtes bien occupés ailleurs. Que font les autres pays chez nous en la matière ?

Enfin, avez-vous des renseignements sur le crash aérien d'aujourd'hui ? Cela peut-il être un acte terroriste ?

M. Bernard Bajolet. Quand survient un attentat, même à l'étranger, faisant des victimes françaises, c'est toujours un échec pour nos services. Nous conduisons alors ce que l'on appelle dans les forces armées un « retex », pour retour d'expérience : nous examinons quels éléments nous avons pu manquer. À côté de l'échec du mois de janvier, il faut savoir que le renseignement intérieur a déjoué bien d'autres attentats. En dépit de toute l'attention consacrée par les services, il est impossible de garantir que nous pourrons toujours empêcher des attentats sur le sol français ou contre nos intérêts à l'extérieur.

A posteriori, on peut se dire que, par exemple, l'un des frères Kouachi ayant séjourné au Yémen, nous aurions pu continuer de le suivre et ainsi empêcher l'attentat. Un des objectifs du projet de loi est justement de nous doter des instruments qui nous permettront de limiter les angles morts, de nous doter de moyens de détection plus performants, sans porter atteinte aux libertés individuelles.

En outre, à la suite de ces attentats, les services ont décidé de se rapprocher davantage. La coopération entre la DGSE et la DGSI était déjà très forte, mais nous allons franchir une étape supplémentaire dans quelques jours, avec l'installation d'une équipe de la DGSE à Levallois-Perret chargée de suivre les filières, sous pilotage de la DGSI. C'est une petite révolution. De même, nous allons transférer à la direction du renseignement militaire (DRM) un certain nombre d'activités dont on peut considérer qu'elles relèvent davantage d'enjeux militaires, afin que chaque service se concentre sur son cœur de métier, pour plus d'efficacité.

En ce qui concerne le renseignement économique, nos concurrents, notamment les plus importants d'entre eux, ne restent pas inactifs vis-à-vis de nos intérêts. Cela suppose une très grande vigilance, en défense. Ces fonctions relèvent essentiellement de la DGSI et de la DPSD pour les industries de défense, en partie de mon service aussi, pour celles des activités nuisibles à nos intérêts économiques menées à l'extérieur du territoire national.

S'agissant de la catastrophe aérienne, je ne peux rien dire à ce stade. L'enquête permettra, je l'espère, de préciser les causes de cet accident.

M. Alain Chrétien. À l'issue de la présentation du projet de loi en Conseil des ministres, quelques associations se sont émues de l'impact que ce texte pourrait avoir sur les libertés publiques. Vos services juridiques ont-ils bien sécurisé ce texte vis-à-vis de la jurisprudence de la Cour européenne des droits de l'homme, laquelle a un pouvoir de plus en plus grand sur ces thématiques, parfois

un peu trop grand d'ailleurs à mon avis, eu égard à la souveraineté des États ? N'y a-t-il pas un risque que cette institution entrave la mise en œuvre de la loi ?

M. Bernard Bajolet. Aussi bien en interministériel qu'au Conseil d'État, la préoccupation de la conventionalité du texte a été constamment présente. La jurisprudence de la Cour européenne des droits de l'homme faisant partie de notre corpus juridique, il est important de s'assurer que nous n'aurons pas de difficultés par rapport à la Convention. Cette préoccupation n'a pas été perdue de vue et je suis donc confiant.

Tout au long des débats, le souci a été de parvenir à un équilibre entre, d'un côté, les besoins des services et la sécurisation juridique de leur activité et, de l'autre, la protection des libertés individuelles. En termes de protection des libertés, je pense que le projet représente une avancée par rapport à la loi de 1991, qui ne prévoyait aucun contrôle pour l'activité de surveillance internationale, en consacrant la jurisprudence qui s'est développée au cours des dernières années. Le point nouveau concerne le recueil de métadonnées pour le suivi de personnes présentant une menace ou la détection de communications caractéristiques d'un réseau terroriste. Dans la mesure où l'anonymat n'est levé qu'en cas de demande d'interception de sécurité, je considère que les garanties sont solides.

Mme la présidente Patricia Adam. C'est aujourd'hui que nous sommes en contradiction par rapport à la Cour européenne des droits de l'homme. Avec la loi, nos concitoyens auront la possibilité de saisir le Conseil d'État, alors qu'aucun recours n'est possible actuellement.

M. Bernard Bajolet. Le recours devant le Conseil d'État est en effet un des points importants vis-à-vis de la jurisprudence de la Cour européenne des droits de l'homme. Il n'existe pas dans le dispositif législatif actuel.

M. Jean-Michel Villaumé. Ne regrettez-vous pas que la coopération internationale, notamment avec les autres services européens, ne soit pas suffisamment évoquée dans le projet de loi ? Il me semble nécessaire de mutualiser les services et les outils au plan européen, pour plus d'efficacité.

M. Bernard Bajolet. Vous avez parfaitement raison sur le fond. Cette coopération européenne existe dans la pratique, mais je ne pense pas qu'un texte de loi soit nécessaire. Cette coopération est plus importante avec les partenaires qui ont des capacités en la matière, notamment l'Allemagne. C'est une priorité, et même une réalité quotidienne.

Mme la présidente Patricia Adam. Cela doit passer par des accords bilatéraux, entre pays, ou multilatéraux, au plan européen. Il reste du chemin à parcourir.

M. Philippe Vitel. Nous avions évoqué ensemble, lors de l'une de vos précédentes auditions, la multiplicité des services de renseignement : six ou sept en France. Le projet de loi améliore la situation de chaque service mais ne traite

pas de leur coordination. Considérez-vous que cette coordination est suffisante ? N'y a-t-il pas lieu, du fait de l'accroissement des menaces, de prévoir davantage de coordination et de mutualisation ?

Par ailleurs, avez-vous parmi vos compétences l'action contre les cybermenaces, et quelles sont vos relations avec l'agence nationale de la sécurité des systèmes d'information (ANSSI) dans ce domaine ?

M. Bernard Bajolet. Il existe un coordonnateur national du renseignement – j'ai été le premier à occuper cette fonction relativement nouvelle. Le projet de loi ajoute une pierre supplémentaire à l'édifice qui s'est construit depuis 2007 avec la création de la délégation parlementaire au renseignement, puis l'année dernière la création de la DGSI… Les événements et la technique nous obligent à davantage de coordination. Les moyens techniques mis à la disposition de la DGSE sont mutualisés, partagés avec les autres services, et font l'objet d'une gouvernance commune, sous l'égide du coordonnateur national du renseignement. Cela dit, les services conservent leur histoire et leur culture propres. Ces cultures différentes présentent aussi des atouts. L'essentiel est d'éviter les duplications et d'agir de façon complémentaire. De ce point de vue, les choses se sont bien améliorées dans le domaine de la lutte antiterroriste, il n'y a pas une feuille de papier à cigarette entre la DGSE et la DGSI. C'est notre devoir de travailler de concert.

M. Jean-Yves Le Déaut. Ayant travaillé sur la sécurité des systèmes informatiques, j'ai vu que la collaboration n'était pas forcément très efficace entre les services spécialisés et ceux qui travaillent en recherche sur ces sujets, et je l'ai écrit, notamment dans des rapports de notre commission. Par ailleurs, j'ai l'impression que l'on n'insiste pas assez sur l'évolution des techniques. L'affaire des survols par des drones l'a montré : nous sommes en retard dans la détection. Un dossier a dû très rapidement être présenté par l'Agence nationale de la recherche, d'un montant d'un million d'euros. Le secrétaire général de la défense et de la sécurité nationale l'a annoncé juste après une audition que nous avions conduite au sein de l'OPECST. Pensez-vous que nous anticipions suffisamment sur ces technologies indispensables ?

M. Bernard Bajolet. Nous nous efforçons d'anticiper et même de créer. Compte tenu de l'importance de nos programmes, nous contribuons à porter de l'avant l'industrie française dans ce domaine. Les techniques évoluent avec une telle rapidité qu'il peut arriver que nous manquions tel ou tel aspect. Au-delà de l'aspect électromagnétique, dont on parle beaucoup, il ne faut pas, vous avez raison, perdre de vue la dimension des images, les drones. On ne doit pas se focaliser sur une technique particulière.

3. Audition de M. Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité (mardi 24 mars 2015).

Mme la présidente Patricia Adam. Nous avons le plaisir de recevoir M. Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), pour une audition sur le projet de loi relatif au renseignement dont notre commission s'est saisie pour avis. Je sais que notre commission vous est moins familière que celle des Lois, monsieur Delarue, et je vous remercie d'avoir répondu à notre invitation.

Le renseignement, l'une des priorités du Livre blanc sur la défense et la sécurité nationale, a fait l'objet d'un long travail avant d'aboutir au texte dont nous allons discuter. Le projet de loi prévoit notamment de faire évoluer l'autorité administrative que vous présidez, qui sera rebaptisée Commission nationale de contrôle des techniques de renseignement (CNCTR). Je vous laisse la parole pour que vous puissiez nous donner votre avis sur ces évolutions.

M. Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Merci, madame la présidente, de votre accueil. Mesdames et messieurs les députés, je suis heureux de pouvoir m'expliquer devant vous sur ce projet de loi, car la commission de la Défense aura un point de vue très utile à faire valoir lors du débat parlementaire.

Avant d'en venir au projet de loi lui-même, je voudrais esquisser les grandes évolutions à venir du monde du renseignement, telles que je les perçois. Tout en sachant que la CNCIS est familière à certains d'entre vous, je voudrais aussi vous dire un mot de sa situation actuelle, ce qui me permettra d'évoquer plus facilement la place réservée au contrôle dans le nouveau texte.

Sur les évolutions du monde du renseignement, je vais m'efforcer d'être à la fois bref et aussi précis que possible. D'abord, et permettez-moi d'y insister puisque c'est mon métier, il faudra veiller à l'équilibre entre les nécessités des services de renseignement et les droits individuels. Cet équilibre doit être respecté de tout temps ; le problème se pose aujourd'hui comme il se posait en 1991, lors de l'adoption de la loi créant la CNCIS. Ensuite, il faudra compter avec la rapidité des évolutions technologiques. Dois-je rappeler que, lorsque vous avez adopté la loi de 1991, internet n'en était qu'à ses balbutiements et que le numérique n'existait pratiquement pas, en tout cas pas sous ses formes actuelles ?

D'autres points méritent d'être mentionnés.

À mes yeux, il y a un effacement de la distinction entre les techniques qui sont intrusives et celles qui ne le sont pas. La loi de 1991 a entériné cette distinction : les interceptions téléphoniques, qui permettent d'écouter des conversations, sont considérées comme plus intrusives que les recueils de données de connexion de téléphones ; elles font donc l'objet d'une vigilance particulière.

Cette distinction va s'effacer parce que, d'une part, les techniques de surveillance deviennent multiples et successives, et que, d'autre part, certaines d'entre elles, qui n'étaient pas nécessairement intrusives au départ, le deviennent par l'emploi qui en est fait. La géolocalisation par repérage des communications téléphoniques permet de situer une personne. Or il n'est pas indifférent de savoir que je suis au cinéma au lieu d'être parmi vous. Les données qui peuvent être recueillies sur une personne forment un tout progressivement indissociable.

La deuxième évolution m'incite à penser que nous avons vécu l'âge d'or des interceptions de sécurité : la cryptologie se répand à grande vitesse et ses procédés deviennent si efficaces que chacun d'entre nous peut avoir recours, pour son ordinateur personnel, à des systèmes qui vont empêcher le service de police intéressé de se saisir de données. Ces procédés devenant à la portée du premier venu, une course s'engage entre la cryptologie et le décryptage.

Troisième élément nouveau : le contrôle consiste à écouter des conversations et à lire leur transcription par les services de police alors qu'à l'avenir il devra porter sur les instruments employés par ces services. Or ces instruments sont de plus en plus compliqués. Pour avoir une vision de ces instruments, il faudra disposer d'une très forte technicité, faute de quoi nous ne contrôlerons rien de ce que voudront faire les services. Le projet de loi qui vous est soumis évoque un instrument qui se branche sur le réseau des opérateurs téléphoniques et qui permettra de faire des analyses. Fort bien. Mais quelle maîtrise aura la CNCTR de cet instrument ? Comment saura-t-elle quels renseignements vont être tirés par les services de ce qu'ils vont brancher sur les réseaux des opérateurs ? Le contrôle va devenir beaucoup plus élaboré.

Dernier point : l'importance de l'international car, si la loi est territoriale, la criminalité et le terrorisme se jouent des frontières. Notre loi nationale doit se positionner par rapport à cette réalité et à des gens qui sont extrêmement mobiles. Dans ce contexte, que sait-on de la nationalité des données numériques ? À peu près rien. Nous sommes devant un droit insaisissable. Que peuvent les services sur ces données ? À qui appartiennent-elles ? On n'en sait à peu près rien. Il faudra régler ces questions.

Sans vouloir insister sur ces perspectives de long terme, je voulais les évoquer avant d'aborder le projet de loi et notamment la situation de la CNCIS, l'organe de contrôle actuel. La CNCIS a été créée par la loi du 10 juillet 1991 pour répondre à une situation de crise, à la suite d'incidents majeurs sur les écoutes téléphoniques. Elle est composée de trois membres, dont deux parlementaires, et présidée par un magistrat. Mon prédécesseur appartenait à la Cour de cassation et, pour ma part, je viens du Conseil d'État. De par sa pratique, cet organe de contrôle a acquis plus de pouvoirs que le législateur ne lui en avait donnés : elle rend un avis préalable alors que la loi ne prévoyait qu'un avis *a posteriori*.

L'image de la CNCIS n'est pas bonne. D'abord, elle est mal connue, ce qui m'est éperdument égal. Surtout, on dénonce souvent sa pauvreté et son

manque de moyens. D'une manière paradoxale, au vu des déclarations de certains anciens responsables policiers après les tragédies de janvier, la CNCIS serait pourtant une empêcheuse de tourner en rond qui gênerait l'action policière. Soulignons cette double lecture.

La Commission joue quatre rôles : elle contrôle les interceptions de sécurité ; elle contrôle *a posteriori* le recueil des données de connexion qui est effectué par une personnalité qualifiée différente ; avec d'autres personnes publiques et sous l'égide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), elle contrôle les matériels de surveillance employés pour s'introduire dans la vie privée des gens ; en vertu de la loi de programmation militaire, depuis le 1er janvier dernier, elle est compétente en matière de géolocalisation en temps réel d'une personne via son téléphone portable. La CNCIS doit donner un avis préalable lorsque les services demandent la géolocalisation en temps réel d'une personne, et elle effectue un contrôle *a posteriori.*

Quelles sont les modalités du contrôle de la CNCIS ? J'aimerais insister sur cet aspect, décisif pour apprécier le projet de loi. Nous contrôlons toutes les demandes qui nous sont présentées, sans exception. Les services le savent et nous entretenons avec eux un dialogue constant et fructueux sur la manière dont ils opèrent. Leurs demandes motivées doivent se rapporter à l'une des cinq finalités prévues dans la loi de 1991 : la sécurité nationale, la prévention du terrorisme, les intérêts économiques essentiels, la reconstitution de mouvements dissous, la criminalité organisée.

En dehors des membres que j'évoquais précédemment, la CNCIS compte trois cadres de la catégorie A. Chacun de nous examine toutes les demandes. Nous procédons ensuite à un échange. Quel avis convient-il de donner ? En cas d'avis favorable, faut-il l'assortir de remarques ? Il nous arrive, par exemple, de raccourcir les délais, le temps que la personne soit identifiée. Quoi qu'il en soit, les décisions sont toujours prises de manière collégiale.

Quels sont nos critères de jugement ? Nous veillons, cela va sans dire, à la légalité, au respect de la loi. Même si la CNCIS n'est pas une juridiction, nous avons aussi, dès sa création, dégagé une sorte de jurisprudence. C'est ainsi que nous avons toujours jugé que l'on ne pouvait écouter les conversations téléphoniques d'une personne que si elle était directement et personnellement impliquée dans une affaire relevant de l'une de cinq finalités précitées. En ce qui concerne les détenus, le délai est toujours raccourci de quatre mois à deux mois car il est facile de judiciariser leur affaire.

Nous faisons évidemment attention aux informations sensibles et nous gardons le secret absolu sur les dossiers. Pour reprendre l'image employée par le président de votre commission des Lois, dans ce pays, on pêche à la ligne et non pas au chalut.

Le Premier ministre est libre de sa décision mais nous représentons en quelque sorte sa garantie contre le risque politique ou pénal d'ordonner une écoute qui ne serait pas légale. C'est sans doute la raison pour laquelle la très grande majorité de nos avis sont suivis, étant précisé que nous donnons peu d'avis défavorables.

Pour terminer par l'essentiel, je signale que nous avons un contrôle *a posteriori* : une fois l'avis préalable donné, nous observons ce qu'il se passe. Tous les produits des écoutes, qu'il s'agisse d'enregistrements ou de transcriptions, sont à notre disposition. À tout moment, il nous est loisible de savoir ce que font les services de l'écoute autorisée. Nous pouvons ainsi savoir si le service remplit les conditions qui lui ont été fixées ou s'il s'en écarte, par exemple en dépassant un délai.

En outre, en cas de demande de renouvellement d'interception, nous saurons si la motivation correspond à la réalité des enregistrements et des transcriptions. C'est pour nous la seule manière de vérifier la sincérité des services. L'autre jour, on nous a soumis une demande motivée par le fait que la personne surveillée se documentait sur les méthodes de torture. En fait, à l'écoute des transcriptions, nous avons entendu l'un des interlocuteurs de cette personne parler des tortures mentionnées dans un livre sur la guerre de 1914-1918 qu'il était en train de lire. C'est un cas d'excès mais les services peuvent pécher par retrait en ne nous disant pas tout ce qu'il faudrait nous dire. Cet accès au contenu des enregistrements et aux transcriptions nous permet donc d'avoir une vue de ce qui se passe mais aussi de la sincérité des services, et c'est très important.

Venons-en au projet de loi. Il me semble qu'il doive obéir à des principes que j'ai définis dans l'avant-propos du dernier rapport annuel que nous avons publié il y a quelques semaines.

Premier principe, que j'ai cité d'emblée : veiller à l'équilibre entre les nécessités de la sécurité et les droits de la personne.

Le deuxième principe, qui découle du premier puisque c'est la condition majeure de l'équilibre, est d'articuler un système à quatre piliers : un service qui fait une demande ; une commission de contrôle qui examine cette demande et rend un avis ; une autorité politique de haut niveau qui prend la décision ; un organisme indépendant des services qui exécute les opérations pour leur compte. En matière d'interceptions, c'est le groupement interministériel de contrôle (GIC), sis aux Invalides, qui s'adresse aux opérateurs et réalise les opérations matérielles nécessaires pour procurer les enregistrements aux services. Cette structure en quatre piliers distincts, voulue par le législateur en 1991, est l'armature essentielle d'un bon système.

Troisième principe : répondre aux besoins des services qui, dans le contexte actuel, sont très importants. Il faut élargir les possibilités techniques – je

précise que je n'ai aucun état d'âme sur ce point – mais, en contrepartie, il faut faire cesser les zones grises ou les illégalités.

Quatrième principe : s'intéresser, même d'assez loin, aux flux internationaux et à ce que peuvent faire les services en dehors de nos frontières.

Cinquième principe : avoir un contrôle indépendant et unifié, c'est-à-dire qu'il faut éviter sa pulvérisation entre différentes instances.

Sixième et dernier principe : le contrôle doit s'exercer *a priori* et *a posteriori.*

Examinons le projet de loi lui-même, au regard de ces principes et pratiques. Il est opportun car le statu quo était impossible, au point même que mes prédécesseurs avaient demandé à plusieurs reprises un nouveau texte pour les raisons que j'ai évoquées, notamment l'évolution technologique.

À ce stade, je voudrais ouvrir deux parenthèses personnelles qui n'engagent pas la Commission. Premièrement, je suis moyennement convaincu par l'argument selon lequel il faudrait une loi sur le renseignement parce que tous les pays démocratiques en ont une. L'organisation des services de renseignement étant essentiellement réglementaire, c'est au Gouvernement qu'il appartient de la définir. Quant au projet de loi, il doit traiter des atteintes aux droits des personnes qui relèvent de l'article 34 de la Constitution, et, éventuellement, de la protection pénale des agents. Deuxièmement, je suis ouvert à la nécessité de donner de nouveaux moyens d'investigation aux services, et il me semble envisageable d'aligner ces moyens de police administrative sur ceux déjà reconnus à la police judiciaire en vertu des articles 100 et suivants du code de procédure pénale.

J'en reviens aux principales conclusions de la CNCIS, consultée par le Gouvernement sur ce projet de loi. J'insiste sur un point : alors que le texte consacre un élargissement sensible des moyens des services et l'augmentation du nombre de personnes susceptibles d'être surveillées, le contrôle n'aura pas les moyens dont il dispose actuellement.

Je ne conteste pas l'élargissement des moyens des services. Qu'en est-il de l'augmentation du nombre de personnes susceptibles d'être mises sous surveillance au moyen d'instruments divers et variés qui vont entrer dans le déroulement de leur vie privée ? Trois dispositions portent sur cette surveillance.

Tout d'abord, l'article L. 811-3 étend très sensiblement les motifs justifiant d'un éventuel recours à des instruments de surveillance, c'est-à-dire aux techniques de renseignement qui sont énumérées dans la loi. Les services spécialisés peuvent notamment y recourir pour le recueil de renseignements relatifs aux « intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France ». Ce point nous préoccupe en ce qu'il permet de viser extrêmement large. Nous n'étions pas opposés à l'extension des motifs, notamment pour couvrir ce que l'on appelle le

hooliganisme, c'est-à-dire les violences répétées et préméditées dans les stades, qui ne relèvent ni de la criminalité organisée, ni d'une atteinte à la sécurité nationale, ni du terrorisme. J'approuve la prise en compte de ce phénomène dans le projet de loi.

Ensuite, les techniques de renseignement employées ne couvrent plus une seule personne ; selon le dispositif employé, la surveillance peut s'étendre à plusieurs milliers de personnes. Prenons trois exemples de surveillance touchant un nombre de croissant de personnes. Dans une pièce d'habitation ou une chambre d'hôtel sonorisée, plusieurs personnes peuvent passer et se trouver ainsi visées. En application de l'article L. 851-7, on pourra aussi utiliser des dispositifs mobiles de proximité pouvant capter, dans un rayon de l'ordre de 500 mètres à un kilomètre, les données de connexion de téléphones et aussi, en cas de terrorisme, les communications elles-mêmes. Supposez qu'un instrument de cette nature soit placé à la gare du Nord où ont transité 190 millions de personnes en 2008. Même en tenant compte du fait qu'il y a des voyageurs réguliers, cette surveillance concernerait un grand nombre de gens… Quant à l'article L. 851-6, il prévoit l'analyse de tout ce qui passe par le réseau d'un opérateur qui couvre des millions de communications. Nul besoin d'épiloguer. L'accumulation supposée admise de ces données nécessitera un tri pour éliminer celles qui sont inutiles à l'enquête et qui peuvent représenter 99,9 % du total. Dans quelles conditions va-t-on éliminer puis détruire ces données inutiles ? L'article L. 822-2 prévoit des délais de conservation très substantiels allant jusqu'à cinq ans pour les données de connexion.

Enfin, le troisième motif d'accroissement du nombre de personnes susceptibles d'être surveillées tient à l'article L. 852-1 qui porte sur les seules interceptions mais nous fait sortir de la jurisprudence sur l'implication directe et personnelle. Cet article prévoit d'autoriser l'écoute de celui qui est soupçonné d'une infraction grave mais aussi de membres de son entourage qui « volontairement ou non » lui servent d'intermédiaire ou peuvent fournir des informations sur l'affaire. Autrement dit, on s'intéresse non seulement à la personne directement impliquée mais aussi à son « relationnel ». Je crains qu'il n'y ait pas beaucoup de limites précises. On pourra ainsi mettre sur écoutes un chauffeur de taxi ayant transporté un trafiquant de drogues. Pourquoi pas, me direz-vous, puisqu'on pourrait tout aussi bien l'interroger dans le cadre d'une enquête de police ? Certes, mais dans le cas d'espèce, les moyens utilisés sont particulièrement intrusifs. C'est toute la différence. Le principe de proportionnalité, que la loi proclame dans ses premiers articles, est-il respecté ? Il doit y avoir un rapport entre la gravité de l'infraction et celle de l'intrusion.

Voilà pourquoi, dans l'avis rendu au Gouvernement, nous nous sommes déclarés préoccupés par cet élargissement.

Tout cela n'aurait peut-être pas trop de conséquences si le contrôle ne se trouvait pas un peu dépourvu, comme nous en avons l'impression. Disant cela, j'ai conscience d'aller à l'encontre de la parole du Gouvernement qui s'emploie à dire

que la CNCTR aura, au contraire, des prérogatives et des moyens supérieurs à la CNCIS. Je crains qu'il n'y ait eu un petit effet d'optique : la CNCIS est réputée pour son peu de moyens, ce que, pour ma part, je n'ai jamais soutenu.

Qu'est-ce qui me permet d'avancer cet argument sur l'affaiblissement du contrôle ? Dans le système actuel, qui repose sur quatre piliers, la CNCIS a accès aux données complètes recueillies par la GIC, donc par les services de police. À l'avenir, toutes les demandes de mise en œuvre de techniques de surveillance ne passeront pas par la CNCTR. Il est notamment prévu une procédure d'urgence absolue qui permet aux services d'envoyer leur demande directement au Premier ministre, sans passer par la CNCTR. Or un service de police peut facilement organiser sa propre urgence absolue.

En outre, certains dispositifs de surveillance ne nécessiteront ni avis de la CNCTR ni même autorisation du Premier ministre. À cet égard, l'article L.851-6 se révèle très compliqué sur le plan des libertés. L'autorisation d'une mesure de localisation en temps réel d'une personne, d'un véhicule ou d'un objet pourra se faire dans les quarante-huit heures. Or les données recueillies doivent être exploitées très rapidement pour ne pas devenir obsolètes et inutiles.

De plus, la CNCTR ne sera pas en état de contrôler les dispositifs techniques employés par les services. On nous annonce que des algorithmes capables de trier les données et de permettre de repérer les personnes ciblées pourront être placés sur les réseaux d'opérateurs. En l'état, faute de disposer de la très forte technicité en informatique nécessaire, je suis incapable de dire si ces algorithmes correspondent effectivement à ce que le service va m'affirmer. Sans compter que pour entrer dans le système mis en place, le service devra me donner lui-même les instruments qui me permettront de le contrôler. Le problème pourra éventuellement être réglé par le recrutement, au sein de la CNCTR, d'informaticiens aux compétences très développées. Je préférerais que cela soit dit.

Enfin, la CNCTR sera dépourvue d'un accès direct aux données. Le projet de loi organise un travail de greffier du GIC et des services, qui devront consigner très scrupuleusement sur des registres ad hoc les mesures exécutées. On pourra trouver la trace des autorisations et de leurs résultats. Mais entre la trace et la réalité, il peut y avoir beaucoup de choses ! Pour fréquenter les services depuis des années, je sais que ces gens font un métier formidable et difficile, mais aussi que le principe de véracité n'est pas ce qu'ils apprennent en priorité. Selon l'article L. 822-1, le Premier ministre veillera à la centralisation des renseignements collectés. Cette disposition m'intéresse énormément tout en me laissant sur ma faim : après avoir entendu des explications orales, j'ai cru comprendre que l'on n'avait pas envie de trop centraliser car ce serait très dangereux pour la sécurité des données. En réalité, il faut sécuriser les locaux.

Pour le reste, la CNCTR devra donc aller à la pêche aux données dans les locaux de chaque service. Actuellement, les enregistrements des transcriptions se

trouvent dans nos locaux. À l'avenir, il faudra aller frapper poliment à la porte des services situés à Levallois-Perret ou boulevard Mortier à Paris. On nous y recevra si on veut. Dans quelles conditions et dans quels délais ? Dans une version antérieure du projet, la CNCTR avait le droit de demander le transport dans ses locaux de certains dossiers, à condition que la vulnérabilité de ces derniers ne soit pas mise en péril. Même si cette disposition était rétablie, il n'en demeurerait pas moins que la vulnérabilité – appréciée par le service – pourrait toujours faire obstacle à la transmission du dossier. La CNCIS tire sa force du fait qu'elle voit tout et dans ses propres locaux.

À mon avis, toutes ces restrictions sont beaucoup plus importantes que les moyens supplémentaires accordés, étant entendu que je ne conteste ni l'intérêt de renforcer les effectifs de la Commission – à vrai dire, je n'en souhaitais pas tant car je pense qu'elle peut être gérée par un petit noyau de gens – ni le recours juridictionnel au Conseil d'État. Tout cela est très important, mais si vous ne donnez pas à la CNCTR les moyens d'avoir prise sur les données brutes du contrôle, vous bâtissez un colosse aux pieds d'argile. Étant un peu expert en matière de contrôle depuis quelques années, je me permets de vous le dire. Si le contrôleur n'a pas accès aux données, il ne contrôlera que ce que l'on voudra bien lui donner et qui ne correspondra pas à la réalité.

Pour conclure, je me réjouis de l'arrivée ce projet de loi qui correspond vraiment à un besoin. Qui s'en plaindrait après les tragédies que nous avons vécues, dans le contexte menaçant que nous connaissons ? Ce texte réaliste part des besoins des services dont certains étaient très demandeurs de légalité. Cependant, nous pensons qu'il faut opérer un petit rééquilibrage.

Mme la présidente Patricia Adam. Les problèmes de contrôle que vous avez soulevés doivent-ils être résolus par des mesures législatives ou par l'octroi de moyens supplémentaires à la nouvelle autorité administrative ?

M. Jean-Marie Delarue. Certaines modifications relèvent à l'évidence de la loi : ce qui a trait au traitement et à la conservation des données, qui sont des informations d'ordre privé ; ce qui peut être fait pour expliciter et compléter l'article L.822-1 sur la centralisation des données par le Premier ministre, en prévoyant notamment un accès de la Commission à ces données ; la suppression éventuelle – que je souhaite – de la procédure d'urgence absolue qui fait l'économie du contrôle par la CNCTR.

En revanche, le Gouvernement peut décider des moyens accordés à la CNCTR. En réalité, je n'ai pas besoin de grand monde sinon de techniciens et d'un nombre suffisant de personnes pour assurer une prise de décision collective. Neuf membres, c'est trop : ils ne vont pas se réunir tous les jours pour suivre les demandes ; ce sont les services qui s'en chargent. La CNCIS – composée en majorité de parlementaires – est chargée de fixer la jurisprudence, un rôle qu'elle a parfaitement tenu depuis 1991. Je souhaite vivement la présence de parlementaires ; on a rajouté des magistrats, ce qui est très bien, mais il me semble

que cinq membres au total suffiraient. La Commission doit compter des spécialistes du droit car nous y jugeons de la légalité de procédures, mais aussi des experts en réseaux informatiques capables d'apprécier la technicité que j'évoquais. Ces dispositions n'ont pas à figurer dans la loi, pas plus que celles concernant la majorité requise pour saisir le Conseil d'État qui me semblent relever du règlement intérieur de la CNCTR. À mon avis, la loi s'immisce un peu trop dans la vie interne de la CNCTR, une autorité indépendante.

M. Philippe Nauche, rapporteur pour avis. Monsieur le président, je vous remercie pour cet exposé qui a le mérite de poser de bonnes questions, même si je ne suis pas sûr que tous les membres de la commission de la Défense partagent vos craintes. Fort de votre expérience, vous plaidez un accès de la CNCTR à toutes les interceptions de sécurité, mais la forte croissance prévisible de leur volume risque de poser un problème.

Vous craignez que le contrôle ne dispose pas des moyens nécessaires à son action. S'agissant de l'article L.852-1 sur la capillarité des écoutes, vous vous interrogez sur le respect du principe de proportionnalité. Pourquoi êtes-vous aussi dubitatif alors que le texte donne à la CNCTR la mission de vérifier cette proportionnalité, via le contrôle des techniques de renseignement ?

Dans le texte, je ne vois pas ce qui vous interdit d'aller à la source dans les services. Cela étant, cette démarche suppose une augmentation des moyens humains de la Commission. À combien estimez-vous les besoins en personnels juridiques et techniques, compte tenu des évolutions de volume de données que vous anticipez ?

Ma dernière question porte sur le recours juridictionnel. Si vous avez le sentiment que l'on vous cache des choses, que le Premier ministre fait systématiquement l'inverse de ce que vous préconisez, vous avez la possibilité d'un recours juridictionnel. Selon vous, si l'on permettait la saisine du Conseil d'État par une minorité des membres de la CNCTR, est-ce que cela offrirait une meilleure protection des droits et des libertés individuelles ou est-ce que cela ne changerait rien ?

M. Jean-Marie Delarue. Vous avez tout à fait raison de penser que nous allons assister à une augmentation très sensible des volumes. Selon le dernier recensement, qui date de 2013, 37 000 données de connexion ont été recueillies dans le cadre de la loi de 2006 sur la prévention du terrorisme et 321 000 l'ont été pour d'autres motifs tels que la criminalité organisée. Signalons que le contrôle d'une donnée de connexion demande relativement peu de temps alors que nous devons nous appesantir quand il s'agit d'interceptions téléphoniques.

Je ne maîtrise pas les flux à venir. Pour la géolocalisation en temps réel, qui a commencé le 1er janvier dernier dans le cadre de l'application de la loi de programmation militaire, nous avions prévu une montée en puissance assez raide. En fait, nous avons reçu moins de 200 demandes depuis trois mois, ce qui est

relativement faible. Les demandes vont certes augmenter au fur et à mesure que les services vont s'habituer à cette mesure, mais elles sont moins élevées que ce que nous avions anticipé. La personnalité qualifiée qui se prononce sur les demandes de données de connexion est installée dans les locaux voisins des nôtres. Son responsable avoue que, certains jours, ils « se battent un peu les flancs ». Malgré ces incertitudes, nous avons évalué à vingt-cinq au maximum, le nombre d'agents collaborateurs nécessaire pour effectuer un travail convenable.

La capillarité est un sujet plus délicat et important. Vous avez raison, la Commission a pour mission de veiller au respect du principe de proportionnalité et elle s'adaptera au texte que vous adopterez. Si vous décidez d'élargir la surveillance aux relations de la personne visée, nous trouverons des jurisprudences pour essayer de bâtir quelques limites. Nous jouerons notre rôle.

M. le rapporteur pour avis. Cet article, qui prévoit d'autoriser l'écoute de membres de l'entourage de la personne soupçonnée, découle aussi de la jurisprudence appliquée par la CNCIS et qui ne figure pas dans la loi de 1991.

M. Jean-Marie Delarue. C'est bien ainsi que je l'ai lu : il va à l'encontre d'une jurisprudence. Actuellement, nous autorisons parfois l'écoute d'un téléphone qui est utilisé de temps à autre par la personne soupçonnée, même s'il s'agit de l'appareil de son épouse. Pour nous, il n'y a pas d'obstacle à l'opération dès lors qu'il existe des indices sûrs d'une association étroite du matériel en question à l'œuvre de préparation d'une infraction grave. Ce projet de loi nous fera sauter un pas supplémentaire alors que, au vu de mon expérience, je ne suis pas sûr que ce soit absolument indispensable pour les services. Certes, les Américains vont beaucoup plus loin puisqu'ils auraient élargi le cercle de surveillance au N +3 – c'est-à-dire à l'entourage de l'entourage de l'entourage de la personne visée – alors que nous n'en serons qu'au N +1. Il faut néanmoins avoir conscience que nous élargissons le cercle des personnes susceptibles d'être suivies.

S'agissant de la saisine directe du Conseil d'État, nous avons cru qu'elle offrait une garantie. La CNCTR ne serait-elle pas encline à s'attendrir devant une décision du Premier ministre et ne faudrait-il pas permettre à seulement deux de ses membres de saisir le Conseil d'État ? Je n'y crois pas trop. D'abord, ce serait blessant pour les parlementaires composant la CNCTR. Ensuite, connaissant un peu les magistrats pour les avoir fréquentés durant quelques dizaines d'années, je serais étonné qu'ils se laissent attendrir par une décision du Premier ministre. Pour ma part, je préférerais que la CNCTR délibère et décide elle-même de la majorité qui permettra une saisine du Conseil d'État. Je ne suis pas sûr que ce soit à la loi de le faire.

Mme Geneviève Gosselin-Fleury. Dans ce projet de loi, notamment dans le volet de lutte contre le terrorisme, est inscrit un dispositif qui utilise le *big data* à des fins préventives et qui aurait notamment recours à un algorithme dit secret pour vérifier les données des opérateurs et détecter des comportements suspects,

mais sous anonymat. Celui-ci ne pourrait être levé que par le Premier ministre en cas de menace avérée. Estimez-vous que cet anonymat est de nature à garantir la protection des libertés individuelles ?

M. Jean-Marie Delarue. À ce stade, il n'y a pas d'autres moyens. J'ai fait part des inquiétudes que m'inspirait cette disposition : en l'état actuel de ses connaissances, la CNCTR est incapable de décrypter l'algorithme en question.

L'un des services de ce pays, que nous connaissons bien, dispose de moyens informatiques extrêmement puissants. J'en suis ravi. Mais lorsque nous allons voir ses instruments, notre intervention relève plus de la contemplation que de l'investigation. Si je dis à ce service que j'ai besoin d'aller voir ce qu'il fait, il va me bâtir un logiciel pour répondre à ma demande. Comment vérifier que ce logiciel répond effectivement à ma demande ?

Au point où nous en sommes, l'anonymat offre en effet une garantie au stade de la collecte des données de connexion d'une masse considérable de gens. Une fois identifiés les numéros de téléphone composés par des terroristes, les personnes appelées seront supposées être elles-mêmes des terroristes. L'anonymat pourra alors être levé sur décision du Premier ministre et gageons qu'un service un peu insistant saura le convaincre.

L'anonymat devient le seul moyen de protéger les libertés individuelles dans un contexte où nous sommes passés à la pratique de la pêche au chalut : nous lançons le filet sans connaître la personne recherchée alors que la pêche à la ligne vise un individu soupçonné, à bon droit ou par erreur, de préparer une action extrêmement grave. L'opérateur de téléphonie ne fabrique pas lui-même le type d'algorithme qui sera placé sur son réseau, sauf pour ses besoins commerciaux. D'où le recours à un dispositif extérieur.

M. le rapporteur pour avis. Pour ma part, je pense qu'il ne s'agit pas tout à fait d'une pêche au chalut telle que pratiquée par l'Agence nationale de sécurité américaine *(National Security Agency, NSA)* qui collecte et stocke toutes les données, dans le cadre de la législation en vigueur outre-Atlantique. Dans le cas présent, il s'agit de déterminer s'il y a matière à organiser une pêche à la ligne un peu démultipliée et non pas de stocker des masses de données qui pourraient être réutilisées un an, deux ans ou trois ans plus tard. Le projet de loi ne prévoit pas un système à l'américaine que nous n'avons d'ailleurs pas les moyens de nous offrir.

M. Jean-Marie Delarue. Puis-je me permettre de vous démentir en partie ? J'ai appelé votre attention, d'une part, sur le tri entre les mauvaises données et les bonnes, et, d'autre part, sur les délais de conservation. Les délais de conservations prévus par la loi, y compris pour les données de connexion, sont de cinq ans – durée à comparer avec les trois ans que vous avez mentionnés. Dans le projet de loi, aucune disposition ne prévoit un tri entre les mauvaises données et les bonnes : nous sommes bien dans la pêche au chalut chère aux Américains.

M. Alain Chrétien. Effectivement, dans ces deux grandes démocraties que sont le Royaume-Uni et les États-Unis, on se pose beaucoup moins de questions qu'en France : le programme Vent Stellaire *(Stellar Wind)* et le système Echelon collectent des données numériques dans le monde entier. En France, les restrictions traduisent peut-être une volonté politique respectable, mais elles résultent aussi des limites imposées par la Cour européenne des droits de l'homme (CEDH) sur lesquelles j'ai interrogé Bernard Bajolet. Les Britanniques se donnent plus de libertés que nous par rapport aux injonctions de la CEDH. Nous devrions nous poser beaucoup moins de questions pour être aussi efficaces que nos collègues anglo-saxons.

Plus précisément, quelle est l'utilité de cette période de quatre mois durant laquelle vous pouvez instruire une demande particulière d'écoute ? Un tel délai est-il compatible avec l'urgence à laquelle vous avez fait allusion ? Il existe une gradation : urgence absolue, quarante-huit heures, deux mois, quatre mois. Ne peut-on pas trouver un système plus flexible qui permettrait aux autorités compétentes d'avoir un avis favorable très rapidement, quel que soit le contexte de la demande ? J'imagine que vous n'allez pas réunir la Commission à deux heures du matin lorsque les services auront besoin d'une autorisation dans l'instant. La délinquance opérant vingt-quatre heures sur vingt-quatre et sept jours sur sept, c'est parfois maintenant ou jamais qu'il faut la ferrer, si j'ose dire pour rester dans le vocabulaire maritime.

M. Jean-Marie Delarue. J'entends bien vos comparaisons entre la Grande Bretagne, les États-Unis et nous, et vos remarques sur le poids de la CEDH que je n'ai pas mentionnée. Sans doute est-ce un élément qui pèse dans le débat public de ce pays. Ce qui m'importe, ce sont les droits de la personne et le respect de la vie privée, qui font partie de notre droit interne.

Venons-en aux délais. Le délai opérationnel dont disposent les services pour mettre en œuvre une mesure est fixé à quatre mois dans le projet de loi qui vous est soumis, tout comme dans la loi de 1991. Quant à la durée d'instruction par la Commission – dont vous vous souciez légitimement en cette période de menaces terroristes – elle varie en fonction du régime appliqué à la demande : en droit commun, nous ne statuons jamais en plus de vingt-quatre heures ; en cas d'urgence absolue, nous ne mettons jamais plus de quarante-cinq minutes à répondre.

Le droit commun correspond à des demandes qui ne nécessitent pas d'urgence particulière. L'urgence absolue s'applique à des demandes qui représentent environ un cinquième du total en année pleine ; en janvier dernier, leur part est passée à 55 % puisque le terrorisme était là.

Nous pouvons statuer jour et nuit. Le président et les services assurent un roulement, vingt-quatre heures sur vingt-quatre et sept jours sur sept, afin de répondre aux demandes individuelles qui leur sont adressées. Ils peuvent réagir d'autant plus vite que la Commission a déterminé la jurisprudence, ce qui leur

permet de ne pas hésiter sur la nature de la décision à prendre. La Commission fixe le cadre et n'entre pas dans les affaires individuelles, ce qui serait résolument incompatible avec l'urgence que vous relevez à fort bon droit. C'est la raison pour laquelle je faisais une réponse un peu nuancée à votre présidente : je ne souhaite pas que la Commission soit trop lourde.

M. Gilbert Le Bris. Sans vouloir nourrir votre réflexion halieutique collective, je dirais que la pêche à la ligne est ciblée, que la pêche au chalut est globale, et que la pêche à la senne fait dans le global ciblé. Dans tout cela, vous devriez trouver ce qui convient. *(Sourires)*

Mais ma question se rapporte plutôt aux deux éléments essentiels qui ont motivé ce projet de loi : l'évolution technologique que l'on ne peut arrêter ; l'augmentation de la menace qui justifie le plan Vigipirate et le déploiement de l'opération Sentinelle. La menace ne semble pas sur le point de se résorber mais, après tout, nous ne sommes pas à l'abri d'une divine surprise. Imaginons une France apaisée, dans laquelle règne la franche camaraderie, le respect des uns envers les autres et la volonté de vivre ensemble, tout cela dans un monde ouvert et lui-même complètement apaisé. Si c'était le cas, si la menace diminuait voire disparaissait, sur quelle mesure faudrait-il revenir en priorité, pour une meilleure protection des droits et libertés individuelles ?

M. Jean-Marie Delarue. Vous évoquez l'évolution technologique. Lorsque le Gouvernement m'avait consulté de façon informelle sur ce projet, il y a bien longtemps, je lui avais recommandé de coller le moins possible à la technologie – pardonnez-moi cette expression triviale – pour que la loi ne soit pas vieille dans six mois ou deux ans. La loi doit s'attacher davantage à définir les modalités d'intrusion dans la vie privée que des dispositifs techniques précis.

Pour le reste, votre question est extrêmement difficile. Même dans le pays que nous appelons tous de nos vœux, il subsistera ce qui fonde la majorité des demandes d'interceptions de sécurité : la criminalité organisée. En temps normal, la criminalité organisée justifie 54 % des demandes d'interceptions, contre 28 % pour la prévention du terrorisme. Au mois de janvier, la prévention du terrorisme a motivé 44 % des demandes, c'est-à-dire pas même la moitié.

Dans un climat apaisé, faudrait-il retirer aux services les moyens techniques dont ils ont légitimement besoin ? Je n'en suis pas sûr. Dans le contexte que vous décrivez, les dispositions concernant la prévention du terrorisme ne trouveraient tout simplement plus à s'appliquer. À cet égard, je ne suis pas mécontent que le Gouvernement ait fait le choix de discriminer les moyens relatifs à la prévention du terrorisme, qui sont sensiblement plus intrusifs que les autres. À l'avenir, il appartiendra au législateur de ne pas étendre à d'autres domaines ces mesures dédiées à la prévention du terrorisme. Il me semble que c'est une manière de répondre à votre question.

Mme la présidente Patricia Adam. Je vous remercie.

4. Audition du général Christophe Gomart, directeur du renseignement militaire (mercredi 25 mars 2015).

Mme la présidente Patricia Adam. Général, mes chers collègues, mesdames et messieurs, je suis heureuse d'accueillir le général Christophe Gomart, directeur du renseignement militaire, pour une audition sur le projet de loi relatif au renseignement.

Nous poursuivons en effet avec vous le cycle de nos auditions sur le sujet, notre commission s'étant saisie pour avis. La direction du renseignement militaire (DRM) fait partie de ce qu'il est convenu d'appeler la communauté du renseignement et comme telle est directement concernée par ce projet de loi. Votre audition nous permettra donc de mieux en comprendre les enjeux.

Général Christophe Gomart. Madame la présidente, mesdames et messieurs les députés, je suis très honoré d'être entendu aujourd'hui par votre commission. Avant de prendre la tête de la direction du renseignement militaire en 2013, j'ai eu la chance de commander les opérations spéciales de 2011 à 2013 ; auparavant, j'ai été adjoint du coordonnateur national du renseignement Bernard Bajolet – de 2008 à 2011 – et chef du bureau réservé du cabinet du ministre à la Défense – de 2006 à 2008. Ce parcours me permet d'avoir une vision assez large du monde du renseignement et de tout ce qui touche à sa spécificité.

Je propose de commencer par vous présenter brièvement la direction du renseignement militaire avant d'évoquer l'état de la menace et ses enjeux majeurs et de conclure par mon appréciation du projet de loi, qui me semble aller dans le bon sens.

Foch disait : « À la guerre, on fait ce qu'on peut avec ce qu'on sait ; pour pouvoir beaucoup, il faut savoir beaucoup ». C'est dans cet état d'esprit que je conçois l'action de la DRM, service de renseignement des armées, à l'heure où nos soldats sont engagés dans de nombreuses opérations à l'étranger et sur le territoire national. Nous contribuons – c'est l'essentiel de mon travail – à l'appréciation autonome de situation des chefs militaires de tous niveaux et des responsables politiques dans le choix des options militaires.

La DRM est l'un des six services de renseignement de notre communauté nationale, au sein de laquelle elle occupe une place particulière liée à ses missions et à son organisation. Service de renseignement des armées, elle est subordonnée au chef d'état-major des armées (CEMA). Elle dépend donc des armées pour l'ensemble de ses ressources humaines, matérielles et financières, et le directeur que je suis est également le conseiller du ministre en matière de renseignement d'intérêt militaire. La DRM est donc un service spécialisé autonome qui agit discrètement, mais pas secrètement. Notre expertise est celle du renseignement d'intérêt militaire, comme l'a rappelé le plan national d'orientation du renseignement (PNOR) 2014-2019, qui est un document secret défense permettant

de définir le périmètre de chacun des services, ce qui me paraît essentiel. Mon périmètre s'intéresse aux parties des forces vives, militaires et paramilitaires, étatiques ou non, de nos adversaires et de leur environnement qui ressortissent strictement aux seuls domaines d'intérêt militaire, c'est-à-dire ayant ou pouvant avoir des conséquences sur nos forces et nos intérêts nationaux. Notre champ d'action est donc large : il couvre aussi bien l'appui direct aux opérations militaires en cours – en Irak, au Sahel, en Centrafrique –, l'anticipation de crises comme en Ukraine ou en Libye, et la veille stratégique permanente comprenant la surveillance des grandes puissances militaires potentiellement dangereuses, notamment la Chine ou la Russie.

Nous relevons ce défi permanent grâce à la nature intégrée de la DRM, qui lui permet de disposer de la gamme complète des capacités nécessaires à l'élaboration du renseignement.

Il s'agit, premièrement, de l'orientation de la recherche, en étant pleinement impliqués dans les travaux du groupe d'anticipation stratégique du chef d'état-major des armées et en favorisant l'exploitation en boucle courte ; deuxièmement, de la recherche du renseignement, car nous disposons – soit en propre, soit du fait de la mise à disposition par les armées – d'un certain nombre de capteurs techniques – électromagnétiques et de l'image – et humains dans tous les domaines ; troisièmement, de l'analyse et de l'exploitation des informations recueillies par le croisement d'expertises géographiques et thématiques ; quatrièmement, enfin, de la diffusion de ce renseignement élaboré aux destinataires idoines.

La DRM est implantée à Paris, Creil et Strasbourg, ainsi que dans neuf centres d'écoute répartis sur la surface du globe. Nous contribuons aussi aux opérations par la projection en permanence d'environ cent personnes sur les théâtres d'opérations. La DRM emploie 1 600 personnes, dont 80 % provenant du personnel de toutes les armées, des services et de la gendarmerie, et 20 % de personnel civil. Nous souffrons, pour la catégorie du personnel militaire, de lacunes dans la réalisation de nos effectifs de personnel de spécialités rares, notamment les interprétateurs images et les linguistes. Les 20 % de personnel civil sont majoritairement des fonctionnaires. Nous avons également la chance de disposer d'agents sous contrat très diplômés, principalement en tant qu'analystes géographiques et thématiques. Notre richesse réside dans cette alchimie d'experts militaires et civils expérimentés ou tout juste sortis d'école.

La loi de programmation militaire (LPM) doit consolider notre capacité de recherche, notamment dans le domaine satellitaire. Nous attendons avec impatience l'arrivée de la constellation MUSIS, prévue pour 2018, et de CERES, qui doit être lancé en 2020. Ces satellites pérenniseront nos capacités stratégiques du renseignement d'origine image et d'origine électromagnétique. Nous sommes aussi vigilants sur la réalisation des autres programmes comme la charge utile de guerre électronique aéroportée pour succéder au C-160 Gabriel, l'acquisition patrimoniale d'avions légers de surveillance et de reconnaissance, comme ceux

que nous louons actuellement sur les théâtres d'opérations et qui se révèlent très efficaces, ainsi que les perspectives de drones MALE en y intégrant une charge de renseignement d'origine électromagnétique (ROEM).

Les attaques du mois de janvier ont cruellement rappelé l'actualité de la menace à laquelle nous sommes confrontés. La DRM s'intéresse principalement à l'adversaire que combattent les armées sur les théâtres d'opérations saharo-sahélien, centrafricain, irakien voire libanais. La zone d'intérêt renseignement est toutefois beaucoup plus vaste que la zone d'opérations *stricto sensu* ; nous avons à regarder aussi ce qui se passe alentour, dans le golfe arabo-persique, au Levant au sens large, en Afrique du Nord et singulièrement en Libye, au Nigeria et au Cameroun pour citer les principales zones chaudes.

Cet adversaire a radicalement évolué au cours de la dernière décennie. La globalisation de la menace qu'envisageaient les deux derniers livres blancs est désormais une réalité dans tous les domaines. Nous faisons face à un ennemi très réactif, résolument moderne, capable de s'adapter à ses adversaires et ayant des objectifs politico-stratégiques bien définis. L'adversaire s'est approprié la révolution mondiale de l'information dans laquelle nous sommes immergés. Il maîtrise parfaitement les moyens en réseau modernes pour recruter, influencer et communiquer. Les publications en ligne ou les vidéos de Daech illustrent combien notre ennemi sait utiliser les failles de nos « sociétés connectées ».

Cette modernité de l'adversaire lui permet aussi d'être très réactif et de s'adapter face à nous sur le terrain. Il combine aisément les modes d'action conventionnels et les modes d'action asymétriques : les groupes armés terroristes (GAT) du Nord Mali montent ainsi des embuscades classiques contre les forces multinationales et continuent de poser des engins explosifs improvisés, tandis que Daech mène des offensives d'envergure en Irak et en Syrie et lance des attaques suicides au cœur même de Bagdad. Connaissant nos restrictions d'action, Daech sait aussi se fondre dans la population, emprunter des tenues des forces de sécurité irakiennes ou entreposer ses armes dans des hôpitaux ou des mosquées. Ayant tiré les enseignements des premiers combats contre la force Serval, les GAT ont revu leurs procédures : ils n'emploient plus les moyens de communication que nous pouvons intercepter et préfèrent désormais se déplacer à moto plutôt qu'en colonnes de *pick-up*.

La continuité de cette menace constitue le fait nouveau qui mobilise l'ensemble des services de renseignement. Les armées combattent cet ennemi « au loin », en Irak et au Sahel, mais cet adversaire est de plus en plus intimement lié avec la menace sur le territoire national que j'évoquais précédemment. Il y a donc une véritable continuité entre l'adversaire qui vient nous attaquer sur le sol national et celui qui se trouve aujourd'hui au Sahel ou en Irak.

Au-delà du constat sur la menace – notre raison d'être –, nous avons aussi à prendre en compte l'évolution de l'environnement dans lequel nous évoluons. Nous avons à faire face à une multiplication des sollicitations et à une croissance

phénoménale des informations à traiter. Lorsque le général Bolelli, mon prédécesseur, s'exprimait devant vous il y a deux ans, la DRM appuyait principalement le théâtre afghan et les derniers soubresauts du théâtre ivoirien ; aujourd'hui, nous sommes engagés sur toute la bande sahélo-saharienne, en Centrafrique, en Irak et au Liban. La réelle explosion du volume d'informations est déjà une réalité et constitue un phénomène qui s'amplifiera dans les années à venir. Il devient donc encore plus difficile de discriminer la bonne information dans une telle masse.

Conscients de ces défis, nous avons engagé la DRM dans un vaste chantier de transformation depuis bientôt deux ans. L'objectif majeur est de garder l'initiative sur notre adversaire. Nous avons pour ambition de continuer à garantir au CEMA sa liberté d'action par sa capacité autonome d'appréciation de situation. Nous revoyons donc en profondeur notre organisation et nos procédures pour les optimiser, les moderniser et les adapter. Nous comptons exploiter pleinement les acquis actuels et futurs des programmes d'équipement de la DRM.

Parmi nos chantiers, je souhaiterais en souligner trois. Premièrement, la DRM dispose désormais d'une capacité de renseignement fusionné géospatial – ce que les Anglo-Saxons appellent GEOINT (*geospatial intelligence*) – au sein d'un centre dédié à Creil, le centre de renseignement géospatial interarmées, véritable *start-up* dont l'ambition est de fournir un renseignement complet, précis, géolocalisé et actualisé sur un support numérique adapté aussi bien aux décideurs stratégiques qu'aux analystes de la DRM et aux chefs militaires tactiques sur le terrain ; il faut voir cela comme une espèce de Google Earth comportant un visualisateur permettant de voir, pratiquement en temps réel, ce qui se passe en tout point du globe.

Deuxièmement, nous poursuivons notre pleine implication dans la mutualisation des programmes entre les services de renseignement. Les moyens de la DGSE, auxquels la DRM, la DGSI, la DNRED et la DPSD ont accès, nous permettent de bénéficier de capacités techniques importantes et dimensionnantes et de guider notre réorganisation.

Troisièmement, enfin, la gestion de la ressource humaine fait l'objet d'une attention toute particulière. Nous avons un besoin criant d'effectifs, au risque d'être asphyxiés et de ne plus répondre correctement aux sollicitations. Ainsi, je ne suis actuellement plus en mesure de suivre les pays classés en catégorie P3, étant obligé de recentrer mes moyens sur les crises actuelles. Nos effectifs ne sont pas pleinement réalisés et nous faisons face à un manque chronique de personnel dans des spécialités importantes, comme les interprétateurs photos et les linguistes. Les enjeux que je vous ai décrits militent pour un renforcement de nos effectifs, afin de nous permettre de traiter cette masse exponentielle d'informations qui nous arrivent et d'y détecter rapidement les signaux d'alerte, capacité vitale pour le renseignement. À titre de comparaison, la DGSE dispose d'un volume de personnel militaire plus important que celui de la DRM – notamment d'un nombre plus important d'officiers brevetés de l'École de

guerre. Il a été décidé, à la suite des attentats, de renforcer les effectifs de 185 personnels pour la DGSE – dont au moins trente militaires, qui n'iront pas forcément à la DRM – et de 65 pour la DPSD. Il faut aussi que nous puissions offrir des perspectives de carrières attractives au personnel, tant militaire que civil. Deux pistes sont déjà explorées mais n'ont pas encore abouti : la recherche d'un statut d'emploi pour notre personnel civil et le développement d'une réelle mobilité interservices.

Nous nous attachons à relever d'autres défis, comme celui de la disposition de systèmes d'information et de communication robustes et résilients, la prise en compte du déménagement vers Balard, en réfléchissant sur les opportunités de stabilité et de cohérence qu'offre la base de Creil où nous sommes déjà implantés, ou encore la consolidation d'un centre de bases de données qui vient de nous être livré.

Je crois aussi que nous devons poursuivre la coopération opérationnelle interservices initiée en appui des opérations en Irak avec la cellule Hermès – dont j'ai souhaité la création, soutenu en cela par le chef d'état-major des armées et le ministre de la Défense –, qui permet à tous les services de renseignement de se retrouver au centre de planification et de conduite des opérations au profit des opérations militaires menées actuellement en Irak. Je suis convaincu que la création d'Hermès, qui constitue une première, nous apportera énormément : elle a tracé la voie d'une plus grande interaction entre les services, d'un échange dynamique et efficace de renseignement au profit de l'action, militaire dans ce cas précis. Les enjeux sécuritaires actuels et futurs, notamment sur le territoire national, militent pour la pérennisation et la consolidation de dispositifs similaires.

À propos du projet de loi relatif au renseignement qui vous est soumis, je souhaiterais faire trois observations liminaires. Premièrement, ce projet colle aux réalités présentes et futures de nos services de renseignement quant à leurs moyens et à leurs missions ; deuxièmement, il donne un cadre clair et applicable à tous les services de renseignement ; troisièmement, je pense que cette loi protégera bien nos citoyens.

Le projet définit les missions des services de renseignement, précise les finalités pour lesquels les services peuvent recourir aux techniques de renseignement prévues par la loi, fixe les techniques de renseignement et leurs conditions de mise en œuvre et définit des procédures de contrôle par une autorité administrative indépendante et par un contrôle juridictionnel.

Pour la DRM, il s'agit d'un projet de loi complet et cohérent qui respecte un équilibre entre les nécessités opérationnelles des services et un contrôle indispensable pour la garantie des libertés publiques. Il assoit aussi la légitimité de l'action des services. Ce projet complète le dispositif existant sans remettre en cause les capacités déjà prévues par les dispositifs législatifs existants.

Les finalités définies dans le titre I[er], pour lesquelles les services peuvent mettre en œuvre les techniques de renseignement, ne contraignent pas la DRM. Dans ce cadre, elle peut remplir l'ensemble de ses missions, de l'appui aux opérations à la veille stratégique.

Il ne fait pas de distinction entre les services qui agissent sur le territoire national et ceux qui agissent à l'extérieur. La DRM agit essentiellement à l'extérieur du territoire national concernant les techniques de renseignement abordées par ce projet. Elle dispose toutefois de capteurs stationnés sur notre territoire : il s'agit notamment des centres d'écoute de Giens et des départements et collectivités d'outre-mer de Mayotte, Pointe-à-Pitre, Papeete et la Tontouta, ainsi que des bâtiments de la marine nationale tels que le *Dupuy-de-Lôme* et d'autres bâtiments embarquant des moyens d'interception électromagnétique. Elle est principalement concernée par les mesures de surveillance internationales et le maintien de celles concernant le spectre hertzien déjà prévues par la loi de 1991.

Pour la DRM, le titre V consacré aux techniques de renseignement soumises à autorisation constitue le principal apport de ce projet de loi. Il définit en effet des dispositions relatives aux mesures de surveillance internationales. Celles-ci prennent en compte la surveillance des communications émises ou reçues à l'étranger à partir de capteurs situés sur le territoire national. Elles tiennent surtout compte de l'évolution des techniques de communications électroniques, qui vont bien au-delà de la simple téléphonie telle qu'elle était définie dans la loi de 1991. Il s'agit d'une avancée importante et indispensable au regard du besoin opérationnel et des nouvelles techniques de communication électroniques.

Le dispositif prévu par ce projet, qui apparaît comme plus souple que celui en vigueur pour les interceptions de sécurité, présente cependant de solides garanties : pour les communications qui renvoient à des identifiants nationaux, leur conservation relève de la même procédure que celle prévue pour les autres techniques de renseignement sous le contrôle de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Par ailleurs, la CNCTR s'assure des bonnes conditions de mise en œuvre de ces mesures.

En son article 5, le projet reprend les dispositions de l'exception hertzienne prévues par l'article 20 de la loi de 1991. La DRM considère que le maintien de ces dispositions est impératif, dans la mesure où le balayage du spectre hertzien à partir de capteurs situés sur le territoire national permet la détection de signaux faibles qui, une fois identifiés, peuvent être traités, par exemple, dans le cadre des mesures de surveillance internationale ou de l'accès aux données techniques de connexion.

Je souhaite souligner deux derniers points qui me semblent importants, car ils permettent aux services de réaliser leurs missions dans de meilleures conditions. Premièrement, les dispositions relatives aux conditions dans lesquelles seront pris les actes réglementaires et individuels concernant l'organisation, la

gestion et le fonctionnement des services, constituent un complément utile au dispositif existant qui vise à garantir l'anonymat des agents ; deuxièmement, l'article 9 du projet, qui complète l'article 41 de la loi de 1978 relative à l'informatique aux fichiers et aux libertés, est une garantie apportée à la nécessaire confidentialité de l'action des services et au respect du secret de la défense nationale face à un contentieux relatif à l'accès aux fichiers, qui s'accroît en permanence.

Enfin, la définition des missions de la nouvelle Commission nationale de contrôle des techniques de renseignement permet une réelle unification des procédures d'autorisation et de contrôle. Elle nous donnera un avis préalable avant la mise en œuvre des techniques de renseignement soumises à autorisation et procédera au contrôle *a posteriori* sur la mise en œuvre de ces techniques. Je pense que l'action de cette commission sera une véritable garantie du respect des libertés publiques.

Le directeur du renseignement militaire que je suis considère donc que ce projet de loi relatif au renseignement concourra au maintien et à l'assurance de l'efficacité des services de renseignements. Notre mission a besoin d'un cadre cohérent appuyé sur des capacités de contrôle. Je salue personnellement cette volonté de nous garantir un tel cadre et je peux vous assurer que l'ensemble des membres de mon service demeurent pleinement engagés dans leur mission, avec pour principale ambition de contribuer à la sécurité de nos concitoyens.

Mme la présidente Patricia Adam. Puisque vous avez évoqué les pays classés dans la catégorie P3, pouvez-vous nous préciser quels sont ces pays ?

Général Christophe Gomart. Nous classons les pays en trois catégories, de la catégorie P1, qui regroupe les pays en crise, ou au sujet desquels la sécurité de la France est directement mise en jeu, à la catégorie P3, constituée de pays que nous estimons présenter un risque plus réduit pour la sécurité nationale – P2 étant évidemment la catégorie intermédiaire. Je précise que nous n'abandonnons pas systématiquement toute surveillance des pays classés P3 : ainsi, nous continuons de suivre de près ce qui se passe dans certains d'entre eux. Compte tenu des contraintes auxquelles nous devons faire face en matière d'effectifs, nous devons cependant cesser de surveiller certains pays, notamment ceux d'Amérique latine et les États-Unis d'Amérique. Nous nous contentons de suivre ces derniers sur les théâtres d'opérations militaires, considérant que la mission militaire de défense basée à Washington est parfaitement en mesure de nous tenir informés sur les chefs militaires américains en poste et leurs orientations.

M. Frédéric Lefebvre. Quelles sont nos relations avec la base de l'OTAN de Norfolk ?

Général Christophe Gomart. Nous avons d'excellentes relations avec le commandant suprême allié Transformation (SACT) et les notes de renseignement

de la DRM alimentent d'ailleurs la réflexion de l'OTAN. En septembre prochain, le général Denis Mercier va succéder au général Jean-Paul Paloméros à ce poste.

La vraie difficulté avec l'OTAN, c'est que le renseignement américain y est prépondérant, tandis que le renseignement français y est plus ou moins pris en compte – d'où l'importance pour nous d'alimenter suffisamment les *commanders* de l'OTAN en renseignements d'origine française. L'OTAN avait annoncé que les Russes allaient envahir l'Ukraine alors que, selon les renseignements de la DRM, rien ne venait étayer cette hypothèse – nous avions en effet constaté que les Russes n'avaient pas déployé de commandement ni de moyens logistiques, notamment d'hôpitaux de campagne, permettant d'envisager une invasion militaire et les unités de deuxième échelon n'avaient effectué aucun mouvement. La suite a montré que nous avions raison car, si des soldats russes ont effectivement été vus en Ukraine, il s'agissait plus d'une manœuvre destinée à faire pression sur le président ukrainien Porochenko que d'une tentative d'invasion.

M. Philippe Nauche, rapporteur pour avis. Je vous remercie de nous avoir fait part de vos convictions au sujet du projet de loi relatif au renseignement et de votre service.

Vous avez indiqué que cette loi collait aux réalités, qu'elle constituait un cadre clair et applicable et présentait des garanties satisfaisantes en termes de garanties des droits des citoyens, et avez insisté sur les mesures de surveillance internationale constituant le cadre général de votre action. Pouvez-vous nous indiquer de quelle manière vous exercez votre droit de suite : les individus et les groupes que vous suivez pouvant être amenés à aller et venir entre la France et l'étranger, assurez-vous le suivi des personnes concernées en tous lieux, ou êtes-vous amenés à passer le relais à un autre service dans certaines circonstances ?

M. Alain Moyne-Bressand. Pouvez-vous nous indiquer comment s'effectue la coordination entre les services civils de renseignement et le vôtre, de nature militaire ? On sait que, par le passé, les relations entre les services de renseignement ont été marquées par une certaine rivalité. La nouvelle organisation va-t-elle vous permettre de travailler la main dans la main, dans l'intérêt de la sécurité et de la République – ce qui doit être une priorité ?

Par ailleurs, on sait que le terrorisme islamiste et extrémiste est à surveiller avec la plus grande attention. Comment vous y prenez-vous pour identifier et suivre les chefs terroristes dans les théâtres d'opérations maliens et irakiens, constitués de régions désertiques et montagneuses extrêmement difficiles d'accès ?

Général Christophe Gomart. La DRM a effectivement vocation à travailler sur les théâtres d'opérations et à assurer la surveillance de tout ce qui est susceptible de constituer une menace pour les forces armées françaises : ainsi

surveille-t-elle ce qui se passe en Libye et peut menacer les troupes déployées au Niger, au Tchad et au Mali. Nous suivons les chefs terroristes et les individus – composant AQMI, par exemple – mais pas forcément les filières, qui relèvent plutôt de la direction générale de la sécurité extérieure (DGSE) et de la direction générale de la sécurité intérieure (DGSI) – cette dernière étant leader.

Le rôle de la cellule interagence Hermès consiste précisément à croiser les renseignements dont disposent ces différents services agissant chacun dans son périmètre. Ainsi la direction nationale du renseignement et des enquêtes douanières (DNRED) suit-elle toutes les filières, de même que TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins), qui observe la circulation des fonds et les éventuelles fermetures de comptes. Les différents services peuvent communiquer entre eux par le biais de la cellule Hermès, mais aussi du coordonnateur national du renseignement, qui réunit les directeurs de service autour de lui au moins une fois par mois, afin que ceux-ci fassent le point sur l'état de la menace et exposent leurs sujets de préoccupation. Il existe donc bien une coordination entre les services, qui revêt un aspect opérationnel d'une part en ce qui concerne Hermès pour le théâtre d'opérations du Levant, d'autre part entre la DGSE, la DRM et le commandement des opérations spéciales (COS) pour le suivi des terroristes du Sahel.

Cette coopération se fait en association avec les Américains, qui mettent à notre disposition des moyens de surveillance aérienne – notamment des drones – afin de suivre des djihadistes devenus plus difficiles à tracer depuis qu'ils n'utilisent plus que très rarement les moyens de communication qui nous permettraient naguère de les localiser. Les terroristes sont donc revenus à des méthodes anciennes – notamment celle de l'estafette – et, en matière de téléphonie, utilisent des dispositifs de courte portée, dont le rayonnement est limité à quelques kilomètres. Ces nouvelles pratiques compliquent considérablement l'interception des communications, ce qui n'empêche cependant pas que certaines actions soient couronnées de succès. Ainsi le COS a-t-il pu neutraliser un certain nombre de chefs djihadistes.

En résumé, il y a bien une coordination entre les différents services, qui ont tous des capacités spécifiques, dépendant des missions qui leur sont confiées.

M. Daniel Boisserie. J'aimerais savoir comment se passe la coopération entre la France et les autres pays d'Europe occidentale. Vous avez évoqué la difficulté à recruter des linguistes et des interprétateurs d'image. Pouvez-vous nous expliquer quel est le rôle des interprétateurs images, et quelle est leur formation ? Pour ce qui est des linguistes, quelles sont les langues les plus recherchées, et celles où vous avez le plus de mal à trouver des personnels ? Enfin, ne pensez-vous pas que la mutualisation des personnels exerçant ces deux fonctions pourrait être plus poussée, notamment en ce qui concerne la DGSE ?

Mme Édith Gueugneau. La DRM fait partie intégrante du système de renseignement français coordonné par le Conseil national du renseignement

(CNR), dont la mise en place en 2008 a permis un meilleur partage des savoir-faire et des informations dans le respect des périmètres de responsabilité de chacun. Quel bilan tirez-vous de la création du CNR ? Aujourd'hui, la France doit se doter de moyens efficaces et modernes, tout en disposant de garanties renforcées et d'une définition forte de la protection de notre nation. Selon vous, comment le projet de loi relatif au renseignement peut-il nous permettre d'aller plus loin face à la menace terroriste dans une société hyperconnectée ?

Général Christophe Gomart. La coopération avec les pays d'Europe occidentale est bonne. La DRM participe à deux forums, dont l'un réunissant régulièrement les pays de l'OTAN autour de divers sujets. Je me souviens que lors de l'un de ces forums, on a cherché à nous forcer la main au sujet de l'Ukraine. Cela montre bien l'importance de disposer de renseignements concrets et factuels : de ce point de vue, la France dispose des moyens lui permettant d'apprécier les situations et de faire valoir son point de vue.

La coopération se fait également dans le cadre de relations bilatérales, c'est-à-dire d'échanges d'informations. La France, généralement très bonne en ce qui concerne l'Afrique, est en mesure de fournir des renseignements sur cette région du monde à ses partenaires, en échange d'autres renseignements concernant des régions où elle en recueille moins. Nous échangeons beaucoup avec les Allemands, les Américains, les Britanniques et les Suisses.

Un interprétateur images est une personne capable de repérer sur une image satellite des éléments que vous et moi ne verrions pas, de déterminer si un missile est érigé ou pas, de mettre en évidence la présence d'un hélicoptère sur la plate-forme arrière d'un navire et d'identifier précisément de quel type d'engin il s'agit, de faire la distinction entre des impacts d'obus et des arbustes, là où tout autre ne verrait que des taches noires. La formation initiale de base dure au moins six mois, et il existe des formations continues complémentaires en vue d'effectuer des analyses encore plus rapides et précises. L'exercice de cette fonction implique une bonne connaissance des capacités adverses, afin de faire la distinction entre les matériels militaires et ceux qui ne le sont pas et d'être en mesure, par exemple, de tirer des conclusions de la façon dont certains canons sont disposés.

Pour former un linguiste en chinois, il faut trois ans ; en russe ou en arabe, deux ans. Nous avons donc tout intérêt à fidéliser les personnels concernés une fois qu'ils sont formés, car la longueur de leur formation constitue un investissement non négligeable. Bien évidemment, nous nous efforçons de mutualiser ces fonctions avec d'autres services de renseignement. Si nous avons actuellement besoin de linguistes maîtrisant le tamasheq – l'une des langues parlées au Sahel –, nous ne savons pas combien de temps il nous sera utile de disposer de tels spécialistes, c'est pourquoi nous y réfléchissons à deux fois avant de faire entrer des personnels dans une filière de formation à cette langue : il est plus judicieux de recourir à des personnels mutualisés. Par ailleurs, quand c'est possible, nous nous efforçons de reconvertir les linguistes spécialisés dans une langue qui ne présente plus un intérêt majeur pour nous : ainsi une partie des

nombreux linguistes que nous avons formés au serbo-croate durant les années 1990 ont-ils été transformés en linguistes spécialistes du russe. De même la crise en Centrafrique nous a-t-elle obligés à trouver des personnes parlant le sango.

Sur ce point, il me semble, à l'instar de mes homologues dirigeant d'autres services, qu'il conviendrait d'engager une vraie réflexion sur le plan national afin de déterminer s'il ne serait pas possible de recruter en France des personnels parlant le tamasheq, le pachto ou le dari – deux langues parlées notamment en Afghanistan –, en contrepartie de la délivrance d'un visa longue durée, voire de l'attribution de la nationalité française. L'un des obstacles auxquels nous nous heurtons en matière de recrutement est que notre service n'est pas forcément celui offrant la meilleure rémunération – et je ne parle même pas des postes proposés par le secteur privé.

Pour ce qui est du projet de loi, je rappelle que la loi de 1991 était intéressante dans la mesure où le législateur avait prévu une grande souplesse, ce qui explique que nous ayons pu attendre jusqu'à maintenant – même si certaines évolutions sont intervenues entre-temps – avant l'élaboration d'une nouvelle loi, rendue nécessaire par les gigantesques progrès accomplis en quinze ans en matière de moyens de communication. L'un des intérêts de la nouvelle loi va consister à rendre légales des actions qui ne l'étaient pas et à protéger les agents qui travaillent pour le bien commun et l'intérêt général. Par ailleurs, cette loi va instaurer un meilleur contrôle, auquel les agents ne cherchent pas à se soustraire : ce sont des gens passionnés qui souhaitent avant tout faire œuvre utile dans le respect des libertés publiques. De ce point de vue, le projet de loi me paraît équilibré, même si des amendements permettront sans doute de préciser certaines choses qui méritent de l'être. Cela dit, cette loi est déjà le fruit d'une longue réflexion, portant la marque d'une fructueuse maturation depuis la loi de 2007 portant création d'une délégation parlementaire au renseignement, et j'y vois une réelle plus-value.

M. Serge Grouard. Vous avez évoqué nos moyens spatiaux, dont j'estime que nous parlons trop peu d'ordinaire, alors que la France est une grande puissance spatiale militaire. Vous avez cité les programmes satellitaires CERES (Capacité de Renseignement Électromagnétique Spatiale) et MUSIS (*Multinational Space-based Imaging System for Surveillance, Reconnaissance and Observation*, ou Système multinational d'imagerie spatiale pour la surveillance, la reconnaissance et l'observation). Pouvez-vous nous confirmer que ces deux programmes seront totalement opérationnels en 2018 ?

Par ailleurs, vous nous avez dit éprouver des difficultés à recruter des interprétateurs images. Le problème réside-t-il dans le fait de peiner à trouver les compétences de base chez les jeunes recrutés, ou dans le fait qu'il ne s'ouvre pas suffisamment de postes ? Dans le premier cas, on peut penser qu'il existe en France des formations qui vous permettraient de recruter des jeunes qualifiés selon vos besoins – à condition que des postes soient ouverts en quantité suffisante, évidemment.

M. Gwendal Rouillard. Vous avez insisté sur la qualité de la coopération mise en œuvre avec nos alliés occidentaux au cours des derniers mois, mais je constate pour ma part que nous avons encore une marge de progression en la matière, en particulier avec les États-Unis, comme on a pu le voir au cours de l'opération Chammal. Pouvez-vous nous dire si des discussions ont été engagées en vue d'une coopération plus efficace – en d'autres termes, afin que nos alliés se montrent plus généreux ?

Général Christophe Gomart. On peut effectivement considérer que, grâce à ses satellites militaires, la France dispose d'une bonne capacité à apprécier les situations : rien ne vaut une image, surtout dans les premiers temps. Pour ce qui est de MUSIS, deux satellites vont être lancés à partir de 2018 – l'un comportant une optique « très haute résolution » (THR), l'autre une optique « extrêmement haute résolution » (EHR). Un troisième satellite doit ensuite être lancé en coopération avec les Allemands, qui participent financièrement au programme. En ce qui concerne CERES, un lancement est prévu pour 2020.

L'imagerie satellitaire française repose actuellement sur les programmes Helios et Pléiades – ce dernier, à vocation partiellement commerciale, accorde cependant une priorité d'accès aux militaires quand ils ont besoin d'images. Helios fournit déjà des images de très haute résolution et demain, nous franchirons une nouvelle étape avec la mise en service de MUSIS en extrêmement haute résolution. Quant aux satellites Pléiades, ils présentent l'avantage de fournir des images couleur, ce qui facilite leur interprétation.

Le flux de recrutement des interprétateurs images n'est effectivement pas suffisant. Le général Denis Mercier, chef d'état-major de l'armée de l'air, à qui j'ai exposé ce problème, a augmenté le recrutement, mais il nous appartient désormais d'ouvrir davantage de postes, ce qui pose un problème de qualification. Face à la pénurie de jeunes disposant de la formation adéquate, je me suis tourné vers le secteur civil afin de savoir comment former de jeunes civils. Tous les stages de formation à la fonction d'interprétateur images – qu'ils aient vocation à exercer au sein des armées, de la DGSE, ou même de l'OTAN – s'effectuent actuellement dans le centre de la DRM de Creil : comme vous le voyez, la France est leader dans ce domaine.

Pour ce qui est du partage de renseignements avec nos alliés, j'insiste sur le fait qu'une telle pratique est toujours compliquée à mettre en œuvre. Pour moi, le renseignement est avant tout national, dans la mesure où il permet à notre pays de disposer de son indépendance en matière de politique étrangère, et à nos dirigeants de prendre des décisions importantes. Pour le directeur d'un service de renseignement, toute la difficulté consiste à déterminer ce qu'il peut communiquer en toute sécurité à ses alliés et partenaires, notamment au vu de leur possible utilisation pour une action militaire.

Pour ce qui est de la coopération avec nos amis américains, la problématique est davantage liée à leur organisation. Lors de mes voyages aux

États-Unis, j'ai eu l'occasion de rencontrer le directeur national du renseignement américain, à qui j'ai clairement dit qu'il devait ouvrir les robinets plus largement s'il voulait obtenir plus de renseignements de la part de la France Pour le moment, les Américains se réfèrent à l'accord dit *Five Eyes*, conclu entre les services de renseignement des États-Unis, de l'Australie, du Canada, de la Nouvelle-Zélande et du Royaume-Uni, et dans le cadre duquel ils partagent beaucoup. Je verrais comme une contrainte le fait d'intégrer ce *Five Eyes*, dans la mesure où cela nous obligerait à partager systématiquement l'intégralité de notre renseignement brut : en l'état actuel des choses, nous n'échangeons avec ces alliés que du renseignement élaboré. Fournir du renseignement brut impliquerait de dévoiler nos capacités – que les Américains connaissent déjà en grande partie, il est vrai.

Au Sahel, les Américains nous donnent tout ce qu'ils ont, et vont jusqu'à mettre à notre disposition leurs drones d'observation équipés de capteurs images et d'interception électromagnétique. Au Levant, ils ont commencé à ouvrir un peu plus les robinets du renseignement, mais beaucoup dépend des commandants de théâtre, qui disposent d'une très vaste marge d'autonomie et peuvent être d'une certaine manière comparés chacun à l'équivalent du CEMA en France. J'ai rencontré Michael G. Vickers, *Under Secretary of Defense for Intelligence*, c'est-à-dire sous-secrétaire à la défense pour le renseignement, qui est très ouvert et m'a expliqué avoir donné des ordres afin que des échanges de renseignements aient lieu. Le problème, c'est que les Français n'apparaissent pas toujours comme un partenaire très fiable aux yeux des Américains : il semble qu'ils nous considèrent comme un peu fantasques, tout en nous reconnaissant un grand professionnalisme et une capacité à agir largement démontrée au Sahel – ce qui les conduit même à admettre qu'ils auraient été incapables d'en faire autant avec si peu de personnel.

Il semble que nous soyons parvenus à enclencher une nouvelle dynamique d'échange, en tenant compte de l'observation des Américains selon laquelle nous ne leur donnions pas suffisamment en retour, donc en revoyant à la hausse le flux de renseignement que nous leur adressons. Pour cela, nous avons dû déterminer de quel type de renseignements ils avaient besoin, et surtout traduire ces renseignements en anglais avant de les leur transmettre. Des officiers de liaison ont été affectés au sein de toutes les structures de commandement américaines impliquées dans la résolution du conflit levantin, au Koweit, auprès de l'unité coordonnant les actions aériennes, à Tampa, et j'ai le sentiment que nous gagnons progressivement la confiance de nos alliés. Petit à petit, nous parvenons à entrer dans leur J2 – l'état-major du renseignement – et à avoir accès aux briefings du *Five Eyes*, auquel nous sommes même parfois associés en un « Five Eyes + 1 » lorsque la France est particulièrement concernée par certains renseignements ou certaines décisions à prendre.

M. Alain Chrétien. Si j'ai bien compris l'esprit du projet de loi relatif au renseignement, vous n'êtes pas très concerné par ses dispositions, puisque votre rôle consiste le plus souvent à suivre des individus de nationalité étrangère en dehors du territoire national. Dans ces conditions, vous pouvez continuer à

pratiquer des interceptions de communications comme vous le faisiez auparavant, sans passer par les fourches caudines de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), qui vous obligerait à emprunter un circuit administratif complexe. Pouvez-vous nous confirmer ce point ?

M. Christophe Guilloteau. Six services de renseignement en France, cela paraît beaucoup, même avec la coordination assurée par la cellule Hermès. Pouvez-vous nous indiquer comment s'effectue le tuilage entre la DRM et la DGSE, en particulier la mutualisation du renseignement avec vos collègues de la DGSE dans le cadre de votre action contre Daech et AQMI ?

Général Christophe Gomart. La DRM semble effectivement moins concernée par la loi sur le renseignement. Point important, le maintien de l'exception hertzienne permet d'intercepter, à partir du territoire national ou de bâtiments de la marine nationale – je pense notamment au *Dupuy-de-Lôme* – des flux émanant non pas de Français, mais de nos adversaires d'aujourd'hui, de demain et d'après-demain. Le SIGINT (*Signals intelligence*, ou renseignement d'origine électromagnétique), comprend à la fois le COMINT (*Communications intelligence*), c'est-à-dire l'écoute des communications transitant par les ondes radio, et l'ELINT (*Electronic intelligence*), à savoir la captation des émissions électromagnétiques d'appareillages électroniques – il s'agit essentiellement des renseignements que l'on peut tirer de l'analyse des émissions radar.

Je ne sais pas s'il y a trop ou trop peu de services de renseignement, puisque d'autres services que les six composant actuellement la communauté nationale du renseignement frappent à la porte pour se joindre à eux. Mes fonctions antérieures d'adjoint du coordonnateur national du renseignement me conduisent cependant à considérer que chacun remplit bien la mission qui lui est confiée. Ainsi la DNRED et TRACFIN présentent-ils une remarquable efficacité en dépit de leur taille modeste. La DGSI résulte de la fusion, en juillet 2008, de la direction de la surveillance du territoire (DST) et de la direction centrale des renseignements généraux (DCRG). La direction de la protection et de la sécurité de la défense (DPSD) agit dans le domaine de la contre-ingérence et de la protection des forces armées du ministère de la Défense et des entreprises travaillant pour la défense. La DGSE est le service de renseignement historique, à vocation générale, qui répond aux besoins du Gouvernement, tandis que la DRM répond à ceux des armées, même si elle éclaire le ministre de la Défense et, *via* le coordonnateur, le chef des armées qu'est le Président de la République. C'est grâce aux renseignements recueillis par ces différents services que l'on dispose aujourd'hui d'une vision large.

Il peut y avoir des frictions entre eux, du fait que certaines de leurs attributions respectives se recouvrent – mais c'est là un inconvénient obligatoire si l'on veut éviter qu'il n'y ait des « trous dans la raquette ». Cela dit, il n'y a plus de guerre des services comme on a pu en connaître par le passé, et le fait de se rencontrer régulièrement autour du coordonnateur, ou de façon bilatérale, favorise une bonne entente. Il existe par ailleurs des protocoles entre certains des services

– il en existe un liant la DRM à la DGSE, et un autre à la DPSD –, régulièrement remis à jour. Nos actions sont donc relativement coordonnées et suivies.

La cellule Hermès joue un rôle intéressant en ce qui concerne la crise au Levant, en ce qu'elle nous amène à mettre en commun ce que nous savons, au profit des formes armées agissant en Irak. Enfin, l'existence de l'Académie du renseignement a un effet positif en ce qu'elle permet aux cadres des différents services de renseignement de se connaître, et de savoir ce que font les uns et les autres. C'est là un aspect très important, car l'organigramme des services de renseignement étant généralement secret, il est très difficile de joindre un interlocuteur au sein d'un service autre que le sien : il n'est évidemment pas question de consulter un annuaire ! Aujourd'hui, grâce aux contacts établis dans le cadre de l'Académie du renseignement, un traitant Afrique de la DRM peut entrer en contact avec son homologue de la DGSE sans trop de difficulté, ce qui n'était pas le cas il y a quelques années.

M. Jean-François Lamour. Vous avez insisté à deux reprises sur la pénurie de personnel et rappelé que, si 185 recrutements avaient été annoncés pour la DGSE et 65 pour la DPSD suite aux événements de janvier dernier, la DRM n'en avait eu aucun, alors que la collecte et le traitement des flux d'information nécessitent d'importants besoins humains, et qu'une centaine de personnels sont présents en OPEX chaque année.

À combien estimez-vous vos besoins aujourd'hui et à moyen terme – notamment dans le cadre de l'actualisation de la loi de programmation militaire – compte tenu du fait que vous servez également de vivier à la DGSE lorsqu'elle souhaite recruter des militaires ?

M. Alain Marty. Pouvez-vous nous faire le point de la situation au Yémen, à savoir quelles y sont les forces en présence et comment vous voyez la situation ? Par ailleurs, avez-vous quelques renseignements concernant l'otage française au Yémen, et une piste au sujet de ses ravisseurs ?

M. Jean-Jacques Candelier. Les événements survenus au cours des dernières années dans le monde ont rendu nécessaire une nouvelle loi sur le renseignement, venant actualiser et compléter la précédente, qui remontait à 1991, sans pour autant porter atteinte aux libertés publiques.

Après l'élimination de Mouammar Kadhafi – que je vois pour ma part comme une erreur, regrettant que les propositions alternatives de l'Union africaine n'aient pas été entendues –, la Libye est devenue un pays ingérable, dont les djihadistes ont fait leur quartier général. En votre qualité de DRM, pouvez-vous nous donner des précisions sur la situation exacte de la Libye, ainsi que sur les rapports entre Daech et Al-Qaïda, que l'on dit tendus ?

Général Christophe Gomart. Pour ce qui est du besoin en personnel, mon rêve serait de pouvoir recruter 300 personnes, ce qui n'est pas tant qu'il y paraît. Comme j'ai eu l'occasion de le dire au chef d'état-major des armées, le

renseignement participe des trois principes de la guerre, à savoir la liberté d'action, l'économie des moyens et la concentration des efforts. Le fait de disposer d'un renseignement de bonne qualité permet une liberté d'action, dans la mesure où il donne les moyens aux chefs militaires et aux décideurs politiques de savoir ce qu'ils vont faire ; il permet d'économiser les moyens en n'engageant que les forces nécessaires, et de concentrer les efforts sur l'endroit précis où se trouve l'adversaire.

Le renseignement ne doit pas être réduit à proportion des effectifs de notre armée : bien au contraire, il doit compenser les réductions d'effectifs de l'armée en permettant d'utiliser au mieux les moyens dont elle dispose : c'est tout l'intérêt du renseignement et de ses capacités d'appréciation autonome des situations. La répartition des missions se fait sous l'égide du coordonnateur, qui rédige un plan national des orientations du renseignement, définissant exactement, selon une vision thématique et géographique, ce qui relève de la responsabilité de chacun des services. Cette répartition, revue annuellement par chacun des cabinets ministériels dont dépendent les services de renseignement concernés, est effectuée de façon rigoureuse.

Le centre de renseignement géospatial interarmées récemment créé nécessite du personnel pour fonctionner de manière satisfaisante, comme tous les nouveaux outils permettant de disposer d'une vision plus réactive et plus précise de ce dont nous avons besoin. Je pense notamment à la recherche en source ouverte, c'est-à-dire au renseignement obtenu par une source d'information publique – aujourd'hui, on trouve pratiquement tout ce que l'on veut sur internet à condition de bien chercher, ce qui nécessite d'importants moyens humains. Le renseignement d'origine source ouverte est très précieux en ce qu'il permet souvent de venir compléter, préciser et recouper le renseignement fermé.

J'aimerais donc pouvoir effectuer 300 recrutements – militaires et civils –, étant précisé que la DRM, dont les effectifs n'ont fait que diminuer au cours des dernières années, emploie actuellement 1 600 personnes, ce en quoi je vois un seuil compte tenu des crises actuelles : nous devons veiller à disposer de capteurs en nombre suffisant pour nous permettre de continuer à exercer notre capacité d'appréciation autonome des situations.

Je ne suis pas chargé du dossier concernant Isabelle Prime, otage française au Yémen – cette affaire est suivie par la DGSE. L'agence de presse Reuters a annoncé par erreur sa libération il y a quelques jours : en réalité, seule l'interprète qui l'accompagnait a été relâchée.

Le Yémen se partage en deux zones : le Nord, où se trouvent les Houthis chiites, et le Sud, territoire des partisans de l'ancien président, réfugié à Aden. L'Arabie saoudite vient de lancer des frappes contre les positions houthies, soulevant des protestations de la part des Iraniens, de plus en plus présents dans le Levant et soutenant à la fois les rebelles chiites, l'armée irakienne et le régime syrien. Les Saoudiens sont particulièrement inquiets, car ils doivent faire face à la

problématique yéménite à leur frontière sud et à la problématique irakienne et de Daech à leur frontière nord.

Nous nous efforçons de suivre ce qui se passe au Yémen, étant précisé que la France a des intérêts importants dans le terminal pétrolier de Balhaf – pour le moment préservé. Le week-end dernier, les Américains ont mené une opération avec les Britanniques afin de procéder au retrait de leurs derniers soldats, stationnés à proximité d'Aden. Nous sommes donc désormais dans le noir car, dans l'impossibilité de recouper sur place les éléments obtenus grâce aux interceptions électromagnétiques et à l'imagerie, il est difficile de disposer d'informations fiables.

Pour ce qui est de la Libye, j'ai participé au Forum international pour la paix et la sécurité en Afrique qui s'est tenu en décembre dernier à Dakar, et je me rappelle que le président tchadien Idriss Déby a longuement insisté sur le fait qu'après avoir créé le désordre en Libye en éliminant le président Kadhafi, l'OTAN devait désormais trouver une solution pour ce pays et son peuple. La situation actuelle inspire une grande inquiétude à mes homologues égyptien et tunisien : Daech commence en effet à s'implanter en Libye, combattant les affiliés à Al-Qaïda après avoir rétabli la division traditionnelle de la Libye en trois wilayas – la Cyrénaïque, la Tripolitaine et le Fezzan – et il serait de l'intérêt des Libyens de s'entendre contre ce troisième acteur. Il est en effet à craindre de voir des combattants de Daech venus du Levant – Irak et Syrie – affluer en Libye afin de prendre possession de certains territoires. On sait que Daech cherche actuellement des ressources financières que la prise des champs pétroliers situés en Irak – dans la région de Kirkouk, où ses hommes ont engagé une offensive – voire en Libye, lui procurerait.

La Libye est déstabilisée, et nous nous inquiétons beaucoup de voir les principaux chefs terroristes d'AQMI s'y trouver – plutôt au nord, tandis que le Sud, notamment la ville d'Oubari, est le théâtre de combats entre les Touaregs et l'ethnie des Toubous, soutenue par Idriss Déby. Plus généralement, la Libye est devenue un lieu où s'affrontent les islamistes et les combattants nationalistes, ces derniers cherchant actuellement à s'emparer de Tripoli, pour le moment sans succès. Enfin, les Égyptiens accueillent en ce moment des avions des Émirats arabes unis destinés à aller bombarder la Libye. L'élimination de Kadhafi a donc effectivement engendré une situation extrêmement complexe, ce qui s'explique en partie par le fait que le dirigeant libyen tenait seul les rênes du pays, qui n'était pas doté de structures étatiques.

5. Audition du général Jean-François Hogard, directeur de la protection et de la sécurité de la défense (mercredi 25 mars 2015).

Mme la présidente Patricia Adam. Je suis heureuse d'accueillir le général Jean-François Hogard. La direction de la protection et de la sécurité de la défense (DPSD) est un des trois services de renseignement relevant du ministère de la Défense. Étant en première ligne dans la mission de protection de nos forces armées, tant en opérations extérieures qu'à l'intérieur, elle est particulièrement concernée, notamment en ce qui concerne la finalité de lutte contre le terrorisme, par le texte dont notre commission s'est saisie pour avis.

Général Jean-François Hogard, directeur de la protection et de la sécurité de la défense. Je vous remercie de me recevoir, à un moment charnière pour le service que j'ai l'honneur de diriger, dans un contexte marqué par des événements dramatiques.

J'ai pris mes fonctions le 1er septembre 2014 après avoir servi dans l'infanterie de marine, principalement dans les troupes aéroportées. J'ai été engagé en Afrique, notamment à la tête de l'opération Licorne en 2009, en Irak et en Afghanistan, en 2003 d'abord, en 2010 et 2011, ensuite, comme commandant de la *task force* La Fayette.

Le 13 février 2013, vous aviez reçu mon prédécesseur, le général Bosser, qui avait présenté la DPSD avec précision. Il ne me semble donc pas utile d'en détailler à nouveau les missions et moyens, sachant que j'ai décidé d'inscrire mon action dans la continuité de celle de mon prédécesseur. J'ai souhaité mener à terme la réforme du service qu'il avait lancée. Le fonctionnement de celui-ci reste complexe, soumis à des impératifs antinomiques comme la circulation interne du renseignement et son nécessaire cloisonnement. Cette recherche de continuité s'entend sans préjudice des réflexions stratégiques, de préparation de l'avenir et d'adaptation à la menace que doit mener constamment tout service de renseignement.

La présente audition s'inscrit dans un double contexte : les travaux en cours relatifs au projet de loi sur le renseignement et les suites des attentats de janvier 2015.

Je commencerai par vous faire part de mon analyse du texte. Celui-ci, vu du service, constitue une avancée majeure. Nous disposerons désormais d'un cadre juridique unifié, cohérent et complet qui renforcera notre efficacité et sécurisera l'action des agents. Je souhaite sincèrement que, par les garanties qu'il instituera, il protège les libertés fondamentales et lève les suspicions qui pèsent parfois sur les services.

Je saisis l'occasion d'exposer mon point de vue sur la question des techniques de renseignement. En effet, les mesures votées auront un impact direct

sur mes capacités opérationnelles, tout particulièrement en matière de lutte antiterroriste.

Je vous apporterai ensuite un éclairage rapide sur la réponse de mon service aux attentats de janvier. Celle-ci éclaire nos besoins pour travailler efficacement. Nous quittons *stricto sensu* la question du projet de loi mais la corrélation est forte entre les deux sujets.

Le projet de loi constituera une avancée pour les missions de la DPSD. Il simplifie, synthétise et unifie un ensemble de textes hétérogènes. Il donne aussi une base solide à l'action des services de renseignement.

Les textes écrits avant le développement exponentiel de l'internet et de la téléphonie mobile étaient devenus obsolètes. Au vu de l'ampleur de la menace, d'une part, et de l'évolution des techniques de communication, d'autre part, il était absolument nécessaire de moderniser le cadre juridique de notre action.

Je souhaite par ailleurs que la loi permette de dédramatiser, de démystifier le rôle des services de renseignement dans notre démocratie, en définissant clairement leurs missions, leurs finalités et les modalités du contrôle de leur action. L'enjeu est autant d'obtenir une avancée juridique fondamentale que d'opérer en France une révolution culturelle. Dans le monde anglo-saxon, le renseignement, admis par la société, bénéficie d'une aura plus positive. Il serait bon que la loi fasse évoluer les mentalités et le regard porté sur les services de renseignement, et qu'elle participe de la diffusion de la culture du renseignement chez nos concitoyens. Ce ne serait pas la moindre de ses vertus.

Le projet de loi me semble également avoir une vertu politique. Il pourrait susciter un débat démocratique sur l'équilibre entre sécurité collective et liberté individuelle, en particulier sur la question de l'emploi de techniques de renseignement. Ce débat est fondamental et ce qui en résultera structurera longtemps nos capacités d'action. En tant que soldat, je suis attaché à la souveraineté de mon pays et à la protection de mes concitoyens. En tant que citoyen, j'appelle de mes vœux un texte équilibré, qui veille aux libertés.

Le débat a déjà commencé dans la sphère publique et médiatique. Un équipement, l'IMSI-catcher, fait controverse. Je souhaite aborder ces questions comme directeur d'un service de renseignement, ne pas éluder certains aspects de mes missions mais aussi en préciser la portée véritable. Surtout, je dois souligner le besoin de mon service en matière de techniques de renseignement. J'entends assurer qu'il en fera une utilisation stricte et mesurée.

L'état de la menace nous impose d'être parfois intrusifs. *In fine*, une menace est toujours incarnée. Derrière les définitions d'ordre général, figurées par la menace terroriste ou l'ingérence économique, nous faisons face quotidiennement et très concrètement à des individus ou des groupes d'individus. Il s'agit de personnes impliquées dans l'organisation d'attentats à venir, se préparant à cibler des communautés, des sites protégés par nos soldats ou les

symboles de nos institutions, mais aussi d'hommes ou de femmes – du stagiaire au membre d'une officine – traités par un service étranger ou missionnés par un concurrent, afin de conduire des actions d'ingérence visant nos industriels de défense, dont ils veulent dérober les secrets et le savoir-faire.

Parfois, l'emploi de techniques de renseignement sur de tels individus est incontournable. Ne pas être intrusif, c'est se priver de la possibilité de suivre de telles cibles – leurs intentions, contacts, complices ou donneurs d'ordres – et de connaître leurs agendas, particulièrement lors d'un passage à l'acte. Ne pas être intrusif en pareil cas, c'est aggraver le risque qui pèse déjà sur nos concitoyens, mais cette intrusion doit être contrôlée et concentrée sur l'adversaire.

J'aborderai cette problématique dans ses aspects les plus concrets. Mon service n'a ni le besoin, ni l'envie, ni les moyens d'utiliser des techniques de renseignement pour un recueil de grande ampleur. Notre besoin porte le plus souvent sur une cible qui a été identifiée comme une menace. Par ailleurs, je veux témoigner de l'éthique de mes personnels, qui constitue un garde-fou, associée à des savoir-faire et savoir-être spécifiques. Je citerai la discrétion et le cloisonnement, le compte rendu systématique à l'autorité, qui renforce le contrôle interne, et le contrôle exercé par la hiérarchie. Enfin, les agents sont formés sur le contenu des lois et règlements en vigueur.

Un service de renseignement doit disposer de moyens techniques de renseignement adaptés aux cibles et à l'époque dans laquelle il vit. Très concrètement, je comprends que le projet donne un cadre juridique à l'emploi des techniques de renseignement dont je pourrais devoir faire emploi, en contrepartie d'un contrôle *ex ante* par l'autorité administrative, la Commission nationale de contrôle des techniques de renseignement (CNCTR). Il permet également d'utiliser, sous le contrôle du Premier ministre, des techniques de renseignement en cas d'urgence absolue, avec un contrôle *ex post* de la CNCTR.

Il me semble donc que le principe retenu à ce stade par le projet de loi est celui du contrôle *a priori* par une autorité extérieure au service – le principe général est celui d'un contrôle par la CNCTR – et ce, même dans le cadre de la procédure d'urgence absolue. Il ne me revient pas de me prononcer sur les modalités que vous retiendrez finalement pour réaliser un contrôle sur les services. Celui-ci est évidemment justifié. Je souhaite simplement qu'il permette de répondre aux cas d'urgence. En tant qu'opérationnel, je sais qu'il faut parfois raisonner en minutes plus qu'en heures. Il faut donc que nous puissions agir dans ces cas qui restent rares.

Outre des techniques que je qualifierais de classiques – les interceptions de sécurité ou les factures détaillées, les « fadettes » –, l'enjeu est de disposer de techniques adaptées à notre temps. L'adversaire lit la presse, écoute la radio, la télévision et consulte l'internet. Il s'informe de nos forces et faiblesses. Il en tire parti et certaines techniques traditionnelles, il faut le reconnaître, deviennent quasi inopérantes.

Il faut aussi s'adapter à la mobilité des cibles, c'est-à-dire non seulement à la mobilité physique, mais aussi à ce que j'appellerais une forme d'agilité numérique. La cible sait varier ses modes et outils de communication. Il est facile d'acheter plusieurs téléphones mobiles ou plusieurs cartes SIM avant de passer à l'acte. Il faut donc que nous complétions les moyens classiques, comme les écoutes administratives, par des moyens techniques tactiques, qui permettent de suivre la cible avec une agilité égale à la sienne.

Ces moyens sont ceux dits de type « R. 226 », en référence à l'article du code pénal fixant les règles de leur utilisation par dérogation, dans un cadre général de prohibition. Il s'agit notamment des IMSI-catchers qui permettent d'identifier, de localiser, voire d'écouter, pour les modèles les plus perfectionnés, un téléphone portable.

Je confirme mon besoin de tels équipements, y compris de la capacité d'interception des conversations. Ce point est fondamental en cas de passage à l'acte imminent, car il est fort peu probable que les autres données de connexion permettent de le détecter. Cependant, les IMSI-catchers ne constituent pas l'alpha et l'oméga du renseignement technique. La mobilité des cibles, leur agilité numérique et leur méfiance face aux écoutes au sens général, nous obligent, si nous voulons être efficaces, à disposer de toute la gamme des équipements adaptés aux fonctions prévues par la loi : capacités en géolocalisation, capacités en sonorisation et capacités de suivre les communications électroniques.

Au-delà de toute considération technique, je confirme que, à terme, je serais en grande difficulté pour remplir mes missions au service de mes concitoyens si je ne pouvais disposer de moyens techniques de renseignement.

Le projet de loi constitue pour notre service une avancée fondamentale. C'est une brique majeure pour engager la transition du service vers une nouvelle phase. Les récents attentats ont en effet révélé qu'il restait des limites à dépasser pour nous adapter pleinement aux menaces.

La crise a définitivement mis en lumière le dimensionnement que doit avoir un service de renseignement. Les attentats ont souligné l'existence de limites structurelles. La difficulté qu'il a fallu dépasser est celle d'une situation de crise, dans le cadre d'un fonctionnement devenu contraint par une logique de temps de paix. Ces limites avaient déjà été identifiées et exprimées dans les études et réflexions stratégiques dont j'ai demandé l'actualisation.

Dès la survenance des événements, la mobilisation du service a été immédiate et générale. L'analyse de la situation s'est traduite par des ordres donnés à l'ensemble des entités du service pour accompagner la montée en puissance du plan Vigipirate puis le déploiement des forces armées sur le territoire national, par des opérations au profit direct de la sécurité de nos forces, de nos concitoyens et de nos entreprises de défense, par des bascules d'effort sur l'activité antiterroriste du service, par l'appel aux réservistes et, parallèlement, par

une analyse des besoins humains et en équipements, transmise à l'autorité politique, qui a attribué soixante-cinq postes supplémentaires dans le cadre du plan antiterroriste, en 2015 et 2016.

Il reste encore un cap à franchir pour relever de nouveaux défis.

La bascule d'effort et l'appel aux réservistes visaient à mieux assurer, dans l'immédiat, certaines missions. L'octroi d'effectifs supplémentaires permettra de pérenniser cet effort. Il s'agit pour moi maintenant de conquérir une ressource humaine rare et disputée.

Dans le cadre de la prolongation du niveau Alerte attentat de Vigipirate, la sécurité de nos 10 000 hommes et femmes déployés relève du défi permanent pour mon service. Chacun d'eux est une cible potentielle. On se rappelle l'agression dont nos soldats ont été victimes à Nice.

La sécurité des hommes s'entend bien entendu sans préjudice de celle des sites ou des installations relevant de ma responsabilité, qu'ils soient publics ou privés. La devise de mon service, « Renseigner pour protéger », prend ici tout son sens.

Le projet de loi sur le renseignement revêt une importance particulière tant il est porteur d'accès à des moyens techniques qui augmenteront notre efficacité en matière d'antiterrorisme, sans toutefois pouvoir se substituer à la ressource humaine, sujet sur lequel nous sommes déjà tous mobilisés dans le cadre de la réactualisation de la LPM. Seule l'intelligence humaine peut faire fructifier les capacités techniques dont nous serons dotés.

Je conclurai sur le projet de loi qui a suscité votre invitation. La loi permettra, je l'espère, des avancées fondamentales. La moindre d'entre elles ne sera sans doute pas de normaliser l'action des services de renseignement dans notre démocratie. Elle fixera les limites voulues par la représentation nationale.

Elle va aussi provoquer un débat de fond, qui a déjà commencé dans la sphère publique et médiatique. J'espère qu'il permettra de dépassionner les questions qui préoccupent légitimement nos concitoyens sur nos missions et nos moyens, et, par extension, sur nos intentions supposées. Je rappelle que ma mission ne peut pas se concevoir sans l'emploi de techniques de renseignement.

M. Philippe Nauche, rapporteur pour avis. Les procédures que le projet de loi confie à la CNCTR vous semblent-elles opérationnelles ? Les garanties qu'elles apportent en termes de libertés publiques permettront-elles à vos services de fonctionner ? Les différentes durées d'autorisation ne créent-elles pas une complexité administrative ? Les procédures d'urgence vous semblent-elles adaptées aux situations particulières ?

M. Joaquim Pueyo. Le projet de loi, qui confie aux services de renseignement la mission de protéger nos intérêts économiques ou scientifiques,

vous permettra-t-il de lutter contre les menaces qui pèsent sur les entreprises ? En tant que citoyen, voyez-vous d'un bon œil le renforcement du rôle de la CNCTR ? Dans votre service, ces nouvelles mesures sont-elles bien acceptées ?

Général Jean-François Hogard. Celles-ci me semblent adaptées. Les différentes durées envisagées ne m'inspirent pas particulièrement d'inquiétude. Elles devraient rentrer rapidement dans les mœurs. Je travaille depuis peu de temps dans le monde du renseignement, mais ceux qui le font depuis des années sont au fait d'une réglementation à laquelle ils se réfèrent chaque jour.

L'honneur des services de renseignement est de savoir parer à l'urgence. Le projet de loi nous permettra de le faire. En dehors du cadre strict des autorisations prévues par le projet de loi, nous n'utiliserons pas ces techniques de renseignement utiles à l'accomplissement au quotidien de nos missions. Je réponds de l'état d'esprit du personnel, que vous avez pu mesurer en vous rendant dans nos services.

Nous veillons sur la sécurité de 10 000 entreprises, dont 4 000 ont accès à des informations ou constituent des sites sensibles, et 2 000 sont liées par contrat avec la défense. Ce secteur met en jeu la souveraineté nationale et la compétitivité de notre économie, dont dépend l'emploi. On ne peut laisser piller des années de travail et des investissements considérables sans protéger les industriels, très demandeurs de cette protection. Le texte nous permettra d'être mieux armés face à des États ou des concurrents dotés de moyens considérables et dénués de scrupules. Demain, nous les affronterons à armes égales.

Le renforcement du contrôle de la CNCTR me semble une bonne mesure. Il lèvera les suspicions que nourrissent ceux qui ne nous connaissent pas. Pour travailler sereinement, il faut établir une relation de confiance entre l'opinion publique, nos services et l'autorité politique qui nous emploie.

M. Alain Chrétien. Vous évoquez à bon escient l'éthique de vos personnels, dont nous louons unanimement le travail. Si, par malheur, il vous arrivait de soupçonner un de vos agents, seriez-vous soumis aux dispositions du projet de loi ou pourriez-vous pratiquer des interceptions sans en référer à votre hiérarchie ?

M. Gilbert Le Bris. Depuis quelques années, nos armées, jadis centrées sur la métropole et les DOM-TOM, et prépositionnées, réalisent plus d'OPEX et travaillent en synergie avec d'autres armées. Ce qui est vrai au niveau fonctionnel l'est plus encore sur le plan institutionnel, du fait de notre réintégration dans le commandement intégré de l'OTAN, où travaillent 800 à 900 militaires français. Au niveau opérationnel, comment réglez-vous les problèmes qui pourraient découler de la porosité entre nos forces et celles d'autres institutions ?

Général Jean-François Hogard. Même si nos équipes partagent une éthique forte, qui les incite à s'autolimiter, on ne peut jamais écarter totalement l'hypothèse qu'une personne s'éloigne du cadre légal. Toutefois, les agents sont

rarement seuls. Il faut vingt personnes pour réaliser une filature. Toute opération est menée avec une autorité sur le terrain et avec plusieurs agents. Dans ces conditions, le dévoiement est difficile. Le cloisonnement, qui constitue parfois une difficulté, car il nous impose d'identifier tous nos interlocuteurs, réduit encore les risques d'écart. Enfin, nous sommes protégés par le fait que nous travaillons sur les supports informatiques où tout est traçable.

Sans doute un agent peut-il soustraire des informations et les transmettre à un concurrent ou à une autre puissance. Cela s'est déjà produit dans le passé. En cas de doute, je n'hésiterai pas à enquêter sur un de mes agents. Mais, d'une certaine façon, nous le faisons déjà quand nous réalisons des contrôles élémentaires ou des habilitations, ce qui est aussi une fonction de la DPSD.

Pour ce faire, nous étudions de près le dossier des agents qui demandent à nous rejoindre. Certains disposent de toutes les compétences requises, comme l'observe notre division des ressources humaines, mais, à regret, nous renonçons à leur collaboration s'ils présentent des vulnérabilités. Par exemple, pour éviter à un de nos agents de subir la moindre pression, nous écartons d'entrée tous ceux qui seraient endettés ou qui auraient noué depuis des années des amitiés personnelles avec des personnes travaillant pour des services étrangers.

M. Alain Chrétien. Pour enquêter sur un de vos agents, devrez-vous vous soumettre à l'approbation de la CNCTR ?

Général Jean-François Hogard. Lorsque je suis amené à enquêter sur l'un de mes agents, je suis soumis au régime d'autorisation instauré par le projet de loi. C'est déjà le cas aujourd'hui. Chargée de la sécurité de l'ensemble du personnel du ministère de la Défense, la DPSD a déjà eu à traiter un cas de ce type.

Nous travaillons de plus en plus avec les armées alliées et les nations de l'OTAN. Nous collaborons avec son représentant contre-ingérence. Nous participons à l'élaboration de la doctrine contre-ingérence des vingt-huit États membres. Des militaires de la DPSD insérés dans les états-majors de l'OTAN veillent à ce que les secrets français soient préservés.

Nous sommes présents à Norfolk, à Mons, à Brunssum, à Izmir et dans d'autres organismes de l'OTAN où des militaires français sont déployés. Comme nous, l'Alliance est très vigilante aux risques de porosité. Dans la lutte antiterroriste, au sein de l'OTAN comme entre États membres de l'Union européenne, on se dit tout, tout de suite. On partage l'information dès qu'un risque est détecté.

Enfin, sur le plan du secret national, les procédures sont très solides. La DPSD veille à détecter et à entraver toute pratique contraire à la réglementation.

M. Gwendal Rouillard. Afin d'assurer toutes vos missions, pourrez-vous redéployer les effectifs de l'échelon central vers les territoires, où votre action est particulièrement appréciée ?

M. Jean-Michel Villaumé. Rencontrez-vous des difficultés pour recruter du personnel qualifié ? Identifiez-vous des besoins de formation dont il faudrait faire part aux écoles militaires ou civiles ?

M. Christophe Guilloteau. Je suis allé chercher sur l'internet des renseignements sur le renseignement. J'y ai trouvé des indications sur votre budget et votre effectif. Au niveau local, comment se fait l'interface entre les services de renseignement ? La mutualisation que prévoit la cellule Hermès vous semble-t-elle efficace ?

Général Jean-François Hogard. La DPSD emploie actuellement un peu moins de 1 100 personnes. Nous avons terminé l'année avec 1 080 personnes.

M. Christophe Guilloteau. J'ai trouvé sur l'internet le chiffre de 1 053 personnes.

Général Jean-François Hogard. Vous avez constaté que le site internet de la DPSD n'est plus accessible. Celui-ci a été momentanément suspendu après les attentats pour parer à la multiplication des piratages contre les sites gouvernementaux. Nous en profitons pour l'améliorer, en veillant à ce que les informations divulguées ne nous affaiblissent pas.

La DSPD employait effectivement 1 053 personnes à la fin de 2013. Son effectif était de 1 076 à la fin de 2014, avec un droit ouvert à 1 079. Notre perspective pour 2015 était fixée à 1 100, maintenant complétée de 45 recrutements supplémentaires, puis 20 en 2016, dans le cadre des renforts du volet antiterroriste accordés par le Premier ministre. Nous emploierons 1 145 personnes fin 2015 et 1 165 fin 2016.

Le service, qui comptait 1 500 personnes en 2008, a donc perdu un effectif important dans le cadre de la révision générale des politiques publiques (RGPP). Je me réjouis que la tendance s'inverse. J'ai lu avec satisfaction que, dans son rapport, la délégation parlementaire au renseignement (DPR) souhaite que notre effectif se monte à 1 300 personnes. C'est à ce niveau que mon prédécesseur avait évalué nos besoins.

Une dynamique positive vient d'être amorcée. Après avoir gagné soixante-cinq postes, nous devrions encore en retrouver quelques-uns, à la faveur de la clause d'actualisation de la LPM. Quand les effectifs globaux ont baissé, l'échelon central a considérablement augmenté les siens au détriment du territorial. Mutualiser certaines fonctions au niveau de la direction centrale était la seule façon de maintenir nos missions avec des effectifs réduits. Nous avons par conséquent centralisé l'exploitation du renseignement, l'appui technique et le soutien, et diminué le nombre de structures hors région parisienne, pour nous

adapter à l'évolution de la carte militaire. Mon prédécesseur a réorganisé la centrale, dont les piliers ont été réduits de six à trois : la stratégie ressources d'une part, les centres nationaux d'expertise, qui traitent les aspects techniques d'autre part, et le cœur du service, c'est-à-dire la contre-ingérence.

À mon sens, on est allé trop loin en diminuant les effectifs sur le terrain. Nous manquons désormais d'inspecteurs de sécurité de la défense (ISD), c'est-à-dire d'agents chargés de recueillir le renseignement. La semaine dernière, j'ai visité un poste situé en province, où se trouvent, en temps normal, deux inspecteurs. Le département ne comprend pas moins de deux régiments, deux centres de la marine nationale liés à la dissuasion nucléaire et une petite base de l'armée de l'air, qui héberge plusieurs radars. Un inspecteur ayant été projeté durant six mois en OPEX, l'autre est demeuré seul en poste pendant cette période. Je n'ai pas constaté sur place de menaces très pesantes, mais il faut manifestement renforcer la capacité en renseignement humain, en analyse et en exploitation. Il faut aussi investir les champs de la technologie moderne, tel que le cyberespace, où nous sommes encore trop peu présents.

Quoi qu'il en soit, nous sommes dans une perspective positive. Je souhaite qu'elle le reste. Je sais pouvoir compter sur votre appui dans ce domaine.

Il semble qu'un IMSI-catcher permette de recueillir toutes les données, mais mon objectif n'est pas celui-là. Il est de suivre une cible. J'ai eu un excellent échange à ce sujet avec M. Delarue, président de la CNCIS, avec lequel j'ai établi une relation de confiance. Selon lui, l'IMSI-catcher permet de « pêcher au chalut ». Pour ma part, je cherche à « pêcher à la ligne ». Je veux m'assurer de manière discrète qu'une cible potentiellement nuisible évolue là où nous pensons.

Nous éprouvons quelques difficultés à recruter des personnes qualifiées. Dans ce domaine, la ressource est rare et disputée. Le Service est en discussion permanente avec la direction des ressources humaines du ministère de la Défense (DRH-MD). En cas de concurrence entre les différents employeurs du ministère, le renseignement est considéré comme prioritaire. Mais les services sont plus regardants en matière de sécurité, ce qui élimine *de facto* des candidatures. Une dernière difficulté tient à la rémunération proposée. Je recrute des cadres de catégorie A débutant à 1 924 euros par mois. Ce salaire n'attire pas un diplômé de sciences-po ou d'une école d'ingénieurs, quel que soit son désir de servir le pays. Nous sommes par ailleurs en concurrence avec le secteur privé. Je note en outre que d'autres services peuvent proposer des salaires plus importants que ceux que je suis en mesure d'offrir. Il faut toute la pugnacité de la sous-directrice de la stratégie et des ressources pour que nous atteignions nos objectifs en matière d'effectifs, comme nous sommes parvenus à le faire en 2014.

Nous disposons d'une petite équipe de formateurs en interne. Trente-deux ISD recrutés lors du dernier concours seront formés durant une année scolaire. Il va de soi que ce type de formation ne peut pas être externalisé. D'autres formations, en revanche, sont mutualisées. L'Académie du renseignement nous

offre des places en formation initiale ou dans les cycles supérieurs. Cette aide crée des ponts entre les services : quand des agents ont passé plusieurs semaines ensemble, ils nouent des liens qui permettent d'accélérer la réaction en cas de crise.

Lorsqu'il m'a fallu chercher rapidement le moyen de passer des informations – à un mauvais moment, car les urgences surviennent toujours le vendredi soir ou le samedi –, j'ai mis à profit les liens que mon chef de cabinet a noués avec la DGSI quand il suivait le cycle supérieur de l'Académie du renseignement. Cela ne m'a pas empêché d'appeler ensuite le DGSI, mais je savais que l'information avait été aussitôt diffusée.

Des besoins de formation se font sentir dans le domaine du cyber. Nous ne trouverons toutes les ressources dont nous avons besoin qu'en recrutant des gens que nous formerons ensuite. Le ministère consent un effort important dans ce domaine. Un pôle est en train de se créer en Bretagne, qui nous permettra, je l'espère, de couvrir nos besoins. Il serait désespérant de ne pas arriver à recruter autant qu'on nous autorise à le faire.

Les interfaces avec nos collègues français sont quotidiennes. Les six services travaillent ensemble : la DGSE (direction générale de la sécurité extérieure), la DGSI (direction générale de la sécurité intérieure), la DNRED (direction nationale du renseignement et des enquêtes douanières), TRACFIN (traitement du renseignement et action contre les circuits financiers clandestins), la DRM (direction du renseignement militaire) et la DPSD.

En France, nous sommes surtout en contact avec la DGSI, la DNRED et TRACFIN, mais nous avons également des liens avec la DGSE et la DRM, notamment à l'étranger. Il nous arrive par exemple de détecter sur le territoire des individus qui avaient été repérés au Yémen et arrivent chez nous en passant d'autres pays, comme le Mali. Le dialogue entre les services permet de suivre ces cibles très finement. L'essentiel est qu'il n'y ait pas de « trous dans la raquette ». Il faut à tout prix éviter qu'une personne détectée comme dangereuse à l'extérieur cesse d'être prise en compte à son retour en France.

Nous avons, plusieurs fois par jour, des échanges sécurisés. Nous recevons les agents des autres services et nous allons les voir. Nous bénéficions de l'appui de TRACFIN et de la DNRED, qui nous apportent une aide considérable. Il s'agit de faire vivre le réseau vertueux des six agences de renseignement, contre les réseaux malveillants, qu'ils soient terroristes, cybernétiques ou financiers. Nous partageons l'intelligence sans laisser d'intervalle à l'adversaire.

Mme Édith Gueugneau. Le rôle de la DPSD en matière de cyberdéfense s'accroît sans cesse, face à la révolution numérique. Comment appréhendez-vous votre mission, quand les supports se multiplient et deviennent de plus en plus petits ?

Quel rôle jouez-vous face à l'administration pénitentiaire, dans la surveillance et la prévention de certains actes terroristes, que les détenus peuvent envisager en lien avec l'extérieur ?

M. Nicolas Dhuicq. Quels liens avez-vous avec le renseignement pénitentiaire, notoirement sous doté ?

Vous dites qu'il ne faut pas laisser de trou dans la raquette. Tout dépend de la taille du tamis. Vous êtes contraints d'effectuer des choix stratégiques, ce qui vous conduit à une vision statistique. Cette situation peut-elle durer longtemps ?

Redoutez-vous les risques d'entrisme ? Nos armées forment en effet de bons combattants et certains pourraient ensuite se servir de leurs compétences pour d'autres fins.

Avez-vous du mal à recruter du personnel qui parle les langues étrangères ? Faut-il attribuer les difficultés des Français dans ce domaine aux défaillances du système scolaire ? Souhaitez-vous formuler des propositions à cet égard ?

Général Jean-François Hogard. Dans le cyber, nous participons à la protection du tissu économique et industriel lié à la défense. Nous intervenons en amont auprès des industriels, en matière de conseil et d'audit. Nous sommes également présents en cas de crise. Lors des attaques informatiques, nous aidons les entreprises à réagir le plus rapidement possible, à prendre des mesures correctrices et à dresser un bilan des données attaquées ou pillées.

Ces missions ne sont pas simples, car nos entreprises, qui suscitent un vif intérêt de la part de leurs concurrents ou des États étrangers, hésitent à prendre toutes les mesures de protection nécessaires, dont le coût rogne leurs marges opérationnelles. C'est particulièrement le cas pour les PME. Nous les aidons à trouver les réponses adaptées à leur cas.

Nous utilisons aussi le cyber, dans le domaine de la contre-ingérence des forces, où nous cherchons à détecter les menaces visant nos unités et le personnel qui y sert. Beaucoup d'informations circulent sur l'internet, notamment sur les réseaux. Nous nous attachons également à identifier l'environnement numérique de nos cibles. Nous possédons une structure interne dédiée, qui monte en puissance. Nous pensons encore progresser, grâce aux soixante-cinq postes obtenus en janvier, et aux effectifs supplémentaires qui pourraient nous être attribués grâce à la réactualisation de la LPM.

Il arrive à d'autres services de judiciariser certains dossiers. Ce n'est pas notre cas. Notre rôle consiste à détecter la menace, puis à transmettre l'information aux services judiciaires. Quand il y a judiciarisation, nous sortons du spectre. S'il n'y a pas lieu de judiciariser mais que la menace existe, nous pouvons l'entraver, par exemple en proposant la révision de son habilitation.

Je comprends l'intérêt que présente un suivi de la population incarcérée. J'ai noté les dispositions du projet de loi à cet égard. Nous avons actuellement une relation, bien qu'elle ne soit pas très forte, avec le monde pénitentiaire. À l'occasion, nous signalons certains individus identifiés comme dangereux. Récemment, un signalement a permis d'éviter l'évasion et le passage à l'acte d'un ancien militaire, incarcéré, qui ne faisait donc plus partie de la population dont nous nous occupons.

Pour faire face à la montée de la menace, j'ai basculé des effectifs sur l'antiterrorisme. Nous nous sommes organisés pour que les mailles du filet soient très fines quand les personnes sont potentiellement dangereuses, et plus larges quand le risque paraît moins fort. Le problème est que nous pouvons nous tromper et que ces personnes évoluent d'une catégorie à une autre. Celles qui nous intéressent ont une capacité d'adaptation redoutable. Elles connaissent nos forces et nos faiblesses. Pour mieux suivre cette population, un renfort substantiel a été apporté, avec les soixante-cinq postes que j'ai évoqués, mais nous devons rester vigilants. Nous réfléchissons beaucoup à la manière d'isoler, avec discernement, les individus dangereux. Nous sommes parvenus à des conclusions intéressantes, mais le travail ne sera jamais terminé. C'est pourquoi j'appelle de mes vœux des renforcements supplémentaires.

La presse signale volontiers les risques d'entrisme. Les quelques anciens militaires qui sont partis dans les filières djihadistes sont des individus qui n'ont bien souvent passé que quelques semaines dans l'Institution et ont été remerciés pour cause d'instabilité ou d'inadaptation à la vie militaire. Il existe dans l'armée une période d'essai de six mois au cours de laquelle l'individu et la hiérarchie peuvent rompre leur contrat à tout moment.

Aucun de ceux qui sont partis à ce stade n'a reçu de formation pointue – par exemple d'artificier ou de tireur d'élite. Il y a, dans le personnel d'active, quelques cas que nous suivons, mais je suis convaincu que les gens n'entrent pas dans l'armée par hasard : ils veulent servir le drapeau français. De plus, l'armée a une forte vertu intégratrice. Quoiqu'hétérogènes – on rencontre chez nous des personnes issues de tous les milieux sociaux et de toutes les origines, ce qui reflète l'évolution de la société, et c'est heureux, –, nos hommes sont patriotes.

Il est toujours difficile de recruter des linguistes, d'autant que notre démarche est spécifique. Les linguistes d'écoute sont spécialisés pour traduire des conversations qu'on leur transmet. Les nôtres sont employés pour faire de l'analyse et à ce titre doivent aussi disposer de capacités en la matière. Nous sommes un petit service qui cible les recherches. Je confirme que nous manquons manifestement de linguistes. Les Français ne sont pas très doués en langue étrangère.

M. Nicolas Dhuicq. Cela tient au système scolaire !

Général Jean-François Hogard. Enfin, notre attention à certains critères de sécurité nous interdit de recruter n'importe quel linguiste.

M. Patrice Verchère. De plus en plus de sites militaires sont survolés par des drones. S'il n'y a pas lieu de redouter d'attaque des petits drones, qui ne peuvent porter des charges importantes, on sent monter une inquiétude. Êtes-vous en mesure d'y répondre ?

M. Daniel Boisserie. Avez-vous le droit de recruter des contractuels, ce qui permet de proposer des salaires plus élevés ? Songez-vous à transférer la DPSD dans une région – pourquoi pas la Bretagne, que vous avez mentionnée – où le coût de la vie est moins cher qu'à Paris ? Enfin, ne pensez-vous que pas le monde du renseignement est encore trop saucissonné ?

Général Jean-François Hogard. La question des drones est délicate. Les citoyens ont l'impression qu'on peut impunément surveiller des sites sensibles. Nous sommes mobilisés sur le sujet, avec les autres services. Nul ne sait qui est vraiment derrière ces survols.

Mme la présidente Patricia Adam. Un agent de la CNIL a été interpellé en flagrant délit … (*Sourires*)

Général Jean-François Hogard. Des journalistes étrangers sont aussi à l'origine de survols de Paris par des drones.

Vous l'avez dit : les petits drones ne constituent pas une menace, et même les plus grands ne peuvent attaquer les sites durcis. Ils peuvent du moins filmer les installations, ce qui n'est pas tolérable. Nous investiguons, tandis que la direction de la protection des installations, moyens et activités de la défense (DPID) réfléchit au moyen de mieux protéger nos installations. Enfin, des études sont menées pour faire évoluer le cadre juridique, ce qui permettra de nous opposer plus efficacement à la menace.

Nous avons le droit de recruter des contractuels, dans un volume déterminé par la DRH-MD. Leur rémunération est moins importante que celle des fonctionnaires : elle se monte à 1 924 euros pour le niveau 1 et à 1 600 pour le niveau 2.

M. Daniel Boisserie. C'est une anomalie. Il doit être possible de mieux rémunérer un contractuel qu'un fonctionnaire, par exemple en lui proposant des primes.

Général Jean-François Hogard. Je ne peux pas leur en accorder. C'est pourquoi il m'est difficile de recruter. J'emploie quelques contractuels, mais ils ne rêvent pas de rester chez moi. Au terme de leur contrat, pendant lequel ils ont acquis une expérience professionnelle, ils sont recrutés par d'autres employeurs qui leur proposent, pour un métier identique ou voisin, un salaire plus élevé.

J’ajoute que nous n’offrons que des contrats précaires, d’un à trois ans renouvelables.

Certains, auxquels nous avons appris le métier, partent au moment où ils deviennent performants. Un ingénieur dans la cyberdéfense est payé 4 500 euros dans le privé, alors que nous ne pouvons lui en proposer que 2 200. Nous recevons beaucoup de *curriculum vitae* de candidats qui ont lu l’article du *Parisien* sur la DPSD, mais il nous est difficile de leur faire une offre attractive. Sans doute reste-t-il la solution de déménager en province.

M. Daniel Boisserie. Les collectivités territoriales qui embauchent un contractuel sont libres de fixer sa rémunération.

Général Jean-François Hogard. Le ministère de la Défense, qui entend maîtriser sa masse salariale, ne nous laisse pas la même liberté. Dans ces conditions, il est difficile de conquérir de la ressource humaine.

6. Audition de M. Jean-Yves Le Drian, ministre de la Défense (mercredi 25 mars 2015).

Compte rendu n° 51 :

http://www.assemblee-nationale.fr/14/cr-cdef/14-15/index.asp

ANNEXE 2

Liste des personnes auditionnées par le rapporteur

Par ordre chronologique

- **M. Renaud Vedel,** conseiller affaires intérieures du Premier ministre ;
- **Mme Agnès Deletang,** conseillère auprès du Conseil national du renseignement ;
- **M. Bernard Bajolet**, directeur général de la sécurité extérieure ;
- **M. Patrick Calvar,** directeur général de la sécurité intérieure, accompagné de **M. Dominique Gilles**, conseiller juridique, et **M. Jean Mafart**, chef du service de l'administration générale ;
- **M. Jean-Claude Mallet**, conseiller auprès du ministre de la Défense, **Mme Claire Landais**, directrice des affaires juridiques du ministère, et **Mme Christine Mounau-Guy**, conseillère politique et parlementaire.