

A S S E M B L É E N A T I O N A L E

X I V ^e L É G I S L A T U R E

Compte rendu

Commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015

- Audition, à huis clos, de M. Didier Le Bret, coordonnateur national du renseignement (CNR) 2
- Audition, à huis clos, de M. Francis Delon, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), accompagné de M. Marc Antoine, conseiller auprès du président..... 20

Mercredi
18 mai 2016
Séance de 16 heures

Compte rendu n°24

SESSION ORDINAIRE DE 2015-2016

**Présidence
de M. Georges Fenech,
Président, puis de
M. Meyer Habib, *Vice-
président***



La séance est ouverte à 16 heures.

Présidence de M. Georges Fenech.

Audition, à huis clos, de M. Didier Le Bret, coordonnateur national du renseignement (CNR).

M. le président Georges Fenech. Nous avons le plaisir d'accueillir M. Didier Le Bret, coordonnateur national du renseignement (CNR), accompagné de Mme Agnès Deletang, magistrate, conseillère juridique auprès du CNR. Merci, monsieur l'ambassadeur, d'avoir répondu à notre demande d'audition.

Nous avons déjà commencé à nous intéresser aux questions qui concernent le renseignement en recevant la semaine dernière les responsables des douanes et de la police aux frontières (PAF). Mais avec vous, comme avec le président de la commission nationale de contrôle des techniques de renseignement (CNCTR) que nous entendrons ensuite, nous allons aborder le cœur même du sujet. Je rappelle que le coordonnateur du renseignement, qui est, selon le Livre blanc sur la défense et la sécurité nationale de 2008, le « point d'entrée des services de renseignement auprès du Président de la République », centralise les informations relatives au renseignement et anime le Conseil national du renseignement, créé en 2008.

En raison de la confidentialité des informations que vous êtes susceptibles de nous délivrer, cette audition se déroule à huis clos. Elle n'est donc pas diffusée sur le site internet de l'Assemblée nationale. Néanmoins, et conformément à l'article 6 de l'ordonnance 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, son compte rendu pourra être publié en tout ou partie, si nous en décidons ainsi à l'issue de nos travaux. Je précise que les comptes rendus des auditions qui auront eu lieu à huis clos seront au préalable transmis aux personnes entendues afin de recueillir leurs observations. Ces observations seront soumises à la commission, qui pourra décider d'en faire état dans son rapport.

Je rappelle que, conformément aux dispositions du même article, « sera punie des peines prévues à l'article 226-13 du code pénal toute personne qui, dans un délai de vingt-cinq ans [...], divulguera ou publiera une information relative aux travaux non publics d'une commission d'enquête, sauf si le rapport publié à la fin des travaux de la commission a fait état de cette information ».

Conformément aux dispositions de l'article 6 précité, je vous demande de prêter le serment de dire la vérité, toute la vérité, rien que la vérité.

M. Didier Le Bret prête serment.

Nos questions vont évidemment tourner autour de la sombre année 2015. Nous sommes d'ailleurs intéressés par votre analyse des différences entre janvier et novembre, à la lumière des retours d'expérience et d'éventuels audits internes réalisés par vos services spécialisés. Quelles leçons en avez-vous tirées ? Qu'est-ce qui, le cas échéant, a fait défaut ? Les cibles étaient-elles trop nombreuses ? La dangerosité de certains individus a-t-elle été mal évaluée ? A-t-on manqué d'informations de la part des services de renseignement étrangers ?

Avec le recul, comment expliquez-vous l'interruption des écoutes des frères Kouachi et d'Amedy Coulibaly, alors même que, selon nombre d'analystes, l'adoption d'un comportement discret est le signe que le passage à l'acte approche ? Comment expliquer que Samy Amimour ait pu quitter le territoire français alors qu'il était sous contrôle judiciaire ?

Pourquoi n'était-il pas surveillé par les services de renseignement ? Comment expliquer qu'Ismaël Omar Mostefaï, qui faisait l'objet d'une fiche S, ait pu lui aussi quitter le territoire ? Comment comprendre que les services de renseignement aient été incapables, tout au long de l'année 2015, de localiser Abdelhamid Abaaoud ?

Aujourd'hui, combien d'individus sont identifiés par les services comme représentant une menace terroriste islamiste et surveillés à ce titre ? Quelle évolution avez-vous observée à cet égard au cours des derniers mois ? Dans quels fichiers leurs noms apparaissent-ils ? Qui les suit ? Ces noms sont-ils partagés avec toute la communauté du renseignement ? Quelle est la valeur ajoutée du nouveau fichier FSPRT (fichier des signalés pour la prévention et la radicalisation à caractère terroriste) ? Sur les 1 000 individus concernés présents sur notre territoire, combien font l'objet d'une procédure judiciaire ? À quel moment décide-t-on de judiciariser ?

Pouvez-vous nous présenter les différentes instances de coordination et de partage des données des services de renseignement en matière d'antiterrorisme ? Quelle est la valeur ajoutée des cellules Hermès et Allat ? Combien de dossiers traitent-elles ? Faut-il aller vers l'interconnexion des fichiers des différents services ? Comment jugez-vous la coopération entre les services de renseignement et les magistrats antiterroristes ? Comment améliorer le recueil d'informations par le renseignement pénitentiaire ? Où en est la collaboration de celui-ci avec les autres services de renseignement, notamment le renseignement territorial et la direction générale de la sécurité intérieure (DGSI) ? Qu'en est-il de la coopération avec les services de renseignement européens, américains, russes ?

S'agissant enfin des moyens, quel premier bilan dressez-vous de l'application des nouveaux articles L. 851-2 – sur le suivi en temps réel d'une liste d'individus – et L. 851-3 – sur les algorithmes – introduits dans le code de la sécurité intérieure par la loi du 24 juillet 2015 ? Les plans de recrutement des services se déroulent-ils correctement ? Le nombre d'arabisants, par exemple, est-il suffisant ?

M. Didier Le Bret, coordonnateur national du renseignement. Je répondrai au fil de l'eau aux questions précises que vous m'avez posées ; si d'aventure j'en oublie, je pourrai y revenir au cours de la discussion qui suivra.

Avant de vous répondre sur le bilan de l'année 2015, j'aimerais, pour éclairer la manière dont nous avons orienté notre action, insister sur la singularité des événements auxquels nous avons assisté alors et jusqu'au premier trimestre 2016, et qui sont à tous égards exceptionnels, voire extraordinaires.

D'abord par leur volume inédit : quatre attaques, dont deux massives ; deux tentatives et six projets déjoués, auxquels se sont ajoutées deux nouvelles attaques au premier trimestre de cette année.

Ensuite, une série de seuils ont été franchis. Le premier a trait à la diversité même des actes qui ont été commis. Nous avons tout eu : des actes d'ampleur, préparés, planifiés, coordonnés – les deux attaques de janvier et novembre ; des actes isolés, perpétrés par des acteurs revenant de théâtres de guerre en Syrie ou par d'autres qui, sans jamais quitter le territoire national, ont pu agir à l'instigation d'un contact sur place ; enfin, des individus relevant de la fameuse catégorie des « loups solitaires » qui, autoradicalisés, ont pris leur décision sur un fondement strictement personnel, mais le plus souvent à partir d'internet, comme, au début de 2016, lors de l'attaque du commissariat de la Goutte-d'Or et de la tentative d'assassinat d'un enseignant juif à Marseille. On retrouve en somme ici toute la typologie qui a été décrite dans la littérature relative au terrorisme.

Le deuxième seuil concerne la progression constante des flux de départs. Certes, celle-ci a enfin, pour la première fois, atteint un palier que nos voisins européens, avec qui j'ai eu l'occasion d'en discuter, ont connu il y a près de six mois. Autrement dit, la croissance des départs a tendance à se stabiliser : c'est une bonne nouvelle. Mais, en 2015, elle a aussi été plus spectaculaire en France que dans tout autre pays concerné : le nombre de Français partis à l'étranger – principalement en Syrie – est passé de 360 en début d'année à près du double, soit 600 personnes, en fin d'année, et à 636 aujourd'hui, ce qui représente une progression, tout à fait insolite, de 62 % en un an.

Un troisième seuil a été franchi dans la furtivité du comportement des terroristes. L'ensemble de la gamme des actions clandestines a ainsi été mobilisé lors des différentes attaques dont j'ai parlé, singulièrement celles de janvier et de novembre : utilisation de filières d'immigration illégale, infiltration de flux de migrants le cas échéant, communications cryptées, cartes bancaires prépayées, recours quasi systématique aux frappes dites obliques, qui consistent à cibler un pays depuis une base arrière logistique située dans un autre pays.

Le quatrième seuil, qui a beaucoup frappé l'opinion publique française, est l'appel aux modes opératoires qui caractérisent un théâtre de guerre – actions kamikazes, usage d'armes de guerre.

Le cinquième seuil concerne la diversification permanente du choix des cibles, qui produit un effet maximal – le fameux effet de sidération, la saturation de nos forces, mais aussi une inquiétude constante touchant l'ensemble des sites potentiellement concernés. Ainsi, dans le cadre de la préparation de l'Euro 2016, les services travaillent en priorité sur les stades – auxquels l'accès peut, on l'a vu, être restreint de manière assez dissuasive – et les *fan zones* ; mais, en durcissant les conditions d'accès à certains sites, on crée nécessairement des cibles « molles » qui peuvent apparaître tentantes à ceux qui cherchent à commettre des actes terroristes. On voit ici à l'œuvre une démarche assez sophistiquée, caractérisée par une faculté de mobilité permanente, dont témoignent la conception d'une attaque multiple comme la capacité de frapper une cible chaque fois différente.

J'en terminerai par le recours massif aux instruments de communication moderne, qui saute aux yeux et fait partie des principales caractéristiques et nouveautés de l'État islamique. Il permet à la fois de toucher un très large public et d'adopter une approche très ciblée, en fonction des relais locaux susceptibles de prendre contact avec les personnes qui se manifestent sur la Toile.

À tous ces éléments, qui étaient peut-être même décelables avant l'année dernière, le Gouvernement a entrepris de répondre dès cette période antérieure à janvier 2015, en tenant compte à la fois de l'échelle du défi à relever et des différents seuils que j'ai évoqués. Le premier aspect engage les personnels, les budgets et les outils.

En ce qui concerne les personnels, dès la fin 2013, au moment où s'est constituée la DGSI, issue de la direction centrale du renseignement intérieur (DCRI), les moyens humains ont été accrus de 432 agents. De même, pour le service central du renseignement territorial (SCRT), 800 postes ont été créés. Je rappelle que la création en 2008 de la DCRI, née de la fusion des renseignements généraux et de la direction de la surveillance du territoire (DST), avait fait perdre 2 000 effectifs à la structure – lesquels ne se sont naturellement pas évaporés, mais ont été transférés ailleurs.

M. le président Georges Fenech. Pardonnez-moi de vous interrompre. Nous aimerions en venir au cœur du sujet : votre mission de coordination, sur laquelle portaient les questions que je vous ai posées concernant votre rôle, les moyens dont vous disposez ou les

raisons pour lesquelles les individus que j'ai cités ont échappé à la surveillance des services. Cela permettra à mes collègues de vous poser ensuite des questions utiles.

M. Didier Le Bret. Je poursuis néanmoins mon propos, si vous m'y autorisez, car j'ai aussi pour mission de conseiller le Président de la République à propos des questions que j'ai commencé d'évoquer, et il me semble important de mesurer le chemin parcouru à cet égard.

Au total, ce sont plus de 2 600 nouveaux personnels qui auront été intégrés à la communauté du renseignement, que je suis chargé d'animer et de coordonner, de 2014 à 2018 – date limite d'exécution du plan de recrutement.

Le budget, en exécution, est passé de 1,242 milliard d'euros en 2013 – pour les six services du premier cercle – à 1,329 milliard en 2015.

Quant aux outils législatifs, que vous connaissez mieux que personne, leur volume est lui aussi exceptionnel. Je citerai la loi de 2012, qui permet de poursuivre les actes de terrorisme commis à l'étranger, la loi de programmation militaire de décembre 2013, qui renforce les moyens d'investigation, la loi de novembre 2014, qui renforce la répression, allonge la liste des infractions, crée le délit d'entreprise terroriste individuelle et permet le blocage des sites internet, enfin les lois de juillet et de novembre 2015, qui définissent le nouveau cadre d'exercice des missions des services de renseignement, leur donnent des outils supplémentaires et permettent de faire profiter les services du deuxième cercle d'instruments auxquels ils n'avaient pas accès auparavant.

J'en viens à vos questions, monsieur le président.

En ce qui concerne la centralisation et la coordination, compte tenu du volume et du flux que j'ai évoqués, il était impératif que l'appareil d'État se dote d'un tableau de bord présentant l'ensemble des signalements. C'était le b.a.-ba du suivi des personnes signalées – principalement, mais pas exclusivement, par le biais de la plateforme créée au printemps 2013 ; il y a eu 14 000 signalements, dont 4 000 venant de la DGSI, le solde se répartissant entre le renseignement territorial, les préfetures et d'autres services. Cette action de centralisation, menée dans le cadre de l'état-major opérationnel de prévention du terrorisme (EMOPT), a permis de constituer le FSPRT, qui permet de savoir exactement qui est suivi par qui, afin d'éviter les doublons et, pire encore, l'absence de traitement par un ou plusieurs services. La réponse est essentiellement déconcentrée : les préfets, avec leurs états-majors, peuvent mobiliser l'ensemble des services de l'État pour réagir à tel ou tel signalement.

Voici l'enseignement majeur que je tire de ce qui s'est passé : le défi que nous avons à relever est la distinction des signaux faibles. Nous ne sommes plus au temps où le nombre de personnes signalées ne dépassait pas quelques centaines, ou plutôt quelques dizaines. Il s'agit donc désormais de concentrer les efforts des services, notamment de la DGSI, sur ce qui fait sens et qui permet d'identifier le passage à l'acte. Je reviendrai sur les différentes réunions du Conseil national du renseignement qui ont été organisées à cet effet.

Au nombre des différentes formes que la coordination a prises courant 2015 figurent Allat et Hermès. Les enseignements que l'on peut tirer de l'expérience ne sont pas identiques pour ces deux plateformes. Allat apporte une véritable valeur ajoutée à la DGSI et à l'ensemble des services : ceux-ci arrivent avec leurs bases de données respectives et interagissent directement en fonction des questionnements et des signalements émanant de la DGSI ou de tout autre d'entre eux. La fonction d'Hermès est d'identifier plus finement les filières à l'étranger, et d'aider la défense et les services concernés à préparer des dossiers

d'objectifs et à étudier les sites qui nous intéressent. Les enjeux sont donc très différents. Pour Hermès, les marges de progression sont réelles, tandis qu'Allat apparaît utile à tous les services que je réunis à ce sujet.

M. Sébastien Pietrasanta, rapporteur. On a l'impression que les structures existent, mais qu'il y en a peut-être trop.

Ainsi, Hermès a été installée par la direction du renseignement militaire (DRM) et par la DGSE, Allat par la DGSI. Mais Allat ne traite que de quelques individus du haut du spectre – elle obtient d'ailleurs des résultats significatifs. Cela pose le problème de l'interconnexion des fichiers.

De même, avec l'EMOPT et l'UCLAT, n'a-t-on pas superposé deux structures chargées à peu près de la même mission ? Est-ce parce que l'UCLAT était mal positionnée au sein de la direction générale de la police nationale (DGPN) que l'on a créé l'EMOPT, rattaché au ministère de l'intérieur ? Pourtant, lorsque l'on interroge les services de renseignement du premier cercle qui ne dépendent pas du ministère de l'intérieur, on s'aperçoit qu'ils ne connaissent même pas l'existence de l'EMOPT, et encore moins celle du FSPRT ! Ils n'y ont pas intérêt, me direz-vous.

Mais pourquoi n'assurerez-vous pas cette mission de coordination et de connexion entre les fichiers ? N'est-ce pas votre rôle de coordonnateur ? Ne pourriez-vous constituer une véritable organisation autonome ? Combien de membres votre équipe compte-t-elle ?

M. Didier Le Bret. Moins de dix : j'ai cinq conseillers.

M. le président Georges Fenech. Mais vous êtes installés à l'Élysée.

M. le rapporteur. N'est-ce pas à vous de coordonner l'ensemble des services, de faire vivre un fichier, d'animer Hermès et Allat ? N'avez-vous pas l'autorité suffisante pour réunir tous les services de renseignement dans une même pièce afin qu'ils mettent en commun leurs fichiers ?

M. Didier Le Bret. L'EMOPT n'a pas d'existence juridique : cette structure a été conçue et créée à partir de l'apport de différents services qui concourent à la lutte contre le terrorisme au sein du ministère de l'intérieur. Il s'agit d'un état-major placé auprès du ministre lui-même, rattaché à son cabinet, et dont le « secrétariat » est assuré par l'UCLAT, si je puis m'exprimer ainsi sans manquer de respect à celle-ci. De l'extérieur, on peut effectivement se demander si les deux structures ne sont pas concurrentes. En réalité, le mérite de l'EMOPT est d'avoir permis d'asseoir tout le monde autour d'une même table, et ce au sein du ministère de l'intérieur. Reste la coordination des services en dehors de celui-ci.

M. le rapporteur. Pour nous en tenir au ministère de l'intérieur, n'aurait-il pas suffi de rattacher directement l'UCLAT au cabinet du ministre, au lieu de créer l'EMOPT ? Vous pouvez me dire le contraire, mais l'EMOPT fait ce qu'est censé faire l'UCLAT. Il se contente de gérer un fichier – et encore, puisque c'est l'UCLAT qui l'administre. On ne comprend pas la répartition des rôles entre l'UCLAT et l'EMOPT. On a l'impression que l'on n'a pas voulu déshabiller l'UCLAT pour habiller l'EMOPT, mais que l'on a contourné la première en créant le second. Qu'en pensez-vous, sans enfreindre votre devoir de réserve ?

M. Didier Le Bret. J'ai interrogé l'ensemble des services directement rattachés au ministre de l'intérieur : ils ont le sentiment d'un progrès...

M. le rapporteur. Avec le FSPRT ?

M. Didier Le Bret. ...ce qui laisse penser que l'UCLAT n'avait peut-être pas l'autorité suffisante pour mener à bien ce travail. En ce sens, la création d'une structure qui, sans la doubler, est directement placée sous l'autorité ministérielle, et dont le fichier est impérativement nourri par tous les services, apparaît comme une amélioration. On aurait peut-être pu faire autrement, mais c'est la décision qu'a prise le ministre.

Le CNR devrait-il coordonner l'ensemble des services, au-delà de ceux qui dépendent du ministre ? D'abord, ces derniers sont déjà nombreux. Je n'irai pas jusqu'à dire que l'essentiel se joue en leur sein, car tous les services doivent être mis à contribution : la DGSE, la direction nationale du renseignement et des enquêtes douanières (DNRED), que vous avez auditionnée, la direction de la protection et de la sécurité de la défense (DPSD), Tracfin, etc. Mais, à titre administratif ou dans le cadre des enquêtes judiciaires, les services sont en grande partie dans la main du ministre de l'intérieur – la sous-direction antiterroriste (SDAT) pour la préfecture de police, la section antiterroriste (SAT) de la préfecture de police de Paris, la sous-direction antiterroriste de la DGSI, et même les services de la gendarmerie. Sans doute le besoin de rationaliser l'approche et la politique publique de contre-terrorisme se faisait-il sentir en interne.

Ma fonction, comme CNR, est de veiller à ce que cette politique publique nationale fonctionne en amont et en aval.

Ainsi, en janvier dernier, s'est tenu sous la présidence du chef de l'État un conseil national du renseignement dont l'un des points principaux consistait à acter le *leadership* de la DGSI dans la définition de la manœuvre globale de lutte contre le terrorisme. Cela peut paraître redondant étant donné la compétence nationale de la DGSI. Néanmoins, c'était la première fois que l'on posait clairement ce principe : c'est la DGSI qui, sous l'autorité du Président de la République et des ministres concernés, donne les orientations majeures à l'ensemble des capteurs de la communauté du renseignement afin de sanctuariser le territoire national. Cette politique pourrait sembler aller de soi à tel ou tel endroit extérieur au territoire, mais l'on part du principe que ce sont les enquêtes de la DGSI qui doivent permettre aux autres services de remonter les différentes filières et de concourir à la manœuvre globale.

La seconde décision entérinée par le conseil national du renseignement consiste à mobiliser l'ensemble des possibilités qu'offre la loi – rien que la loi, mais toute la loi –, notamment les deux articles que vous avez mentionnés, monsieur le président, afin d'aider la DGSI à faire son travail de discrimination, en créant des ETP et en formant des analystes capables de traiter la matière brute recueillie par les différents services, dont la DGSE, grâce à ces nouvelles dispositions législatives.

Tout cela se met en place. C'est compliqué, car la loi définit très précisément ce qui est permis. Ainsi, le suivi renforcé instauré par l'article L. 851-2 concerne les seuls terroristes qui représentent une menace. Il va donc falloir travailler sur les textes pour voir jusqu'où nous pouvons aller, par le dialogue et grâce à la compréhension qu'en a la CNCTR, afin que la DGSI puisse disposer de ces outils pour distinguer, au sein des 14 000 signalements, ce qui fait sens et permet de remonter les filières et d'identifier les comportements à risque.

M. le rapporteur. Avez-vous le sentiment que la coordination entre nos services a été suffisante au moment des attentats ? Y a-t-il eu un problème d'échange d'informations ? Que pensez-vous de notre coopération avec les services de renseignement étrangers, notamment européens et turcs ? Enfin, aujourd'hui, la coordination entre nos services peut-elle encore progresser ou est-elle parfaitement satisfaisante, notamment grâce à Allat et à Hermès ?

M. Didier Le Bret. On peut toujours progresser. Peut-être ces deux cellules préfigurent-elles une mutualisation accrue des moyens. Nous avons en France une organisation particulière, héritée de l'histoire, qui a accumulé plusieurs strates de politique publique en matière de renseignement. Certains pays ont fait d'autres choix, par exemple celui de plateformes techniques au service de l'ensemble de la communauté ; chez nous, c'est la DGSE qui intègre une direction technique puissante, laquelle doit elle aussi servir l'ensemble de la communauté.

L'évolution du système demande du temps. À supposer que je puisse exploiter demain, grâce aux outils de la DGSE, toutes les données qui intéressent la DGSI, il n'est pas certain que celle-ci dispose, malgré les efforts consentis depuis plusieurs années, de la capacité d'analyser ces données brutes qui, en tant que telles, ne signifient rien. Évitions le fétichisme du *data mining* (exploration des données) qui voudrait qu'en mettant 14 000 sélecteurs dans une machine on puisse savoir quand, comment et à quelle heure va se produire le prochain attentat ! Au mieux, nous parviendrons à des triangulations, à des éléments concernant l'environnement d'individus dont nous ne connaissons pas les relations auparavant, ce qui nous permettra d'affiner notre approche.

M. le rapporteur. Pour vous, il n'y a eu en 2015 aucun problème de coordination entre les services, aucun « trou dans la raquette » ?

M. Didier Le Bret. Je ne peux vous l'affirmer : il y a toujours des « trous dans la raquette ».

M. Meyer Habib. Le résultat, c'est que nous n'avons pas été bons.

M. Didier Le Bret. Dès lors que nous avons été frappés, il faut dire que nous n'avons pas été bons. Mais nous n'avons pas été frappés entre 1996 et 2012.

La menace a changé, je l'ai montré, et nous avons pris une série de mesures en conséquence.

Pour lutter contre le terrorisme, la mutualisation des données doit être la norme, et non l'exception, et il faut échanger en temps réel, car le temps joue toujours contre nous. C'est le choix qu'ont fait certains pays au lendemain du 11 septembre 2001. Entre le 11 septembre, les attentats de 2004-2005 en Espagne et au Royaume-Uni et l'année 2012, il n'y a pas eu beaucoup de réformes de structure en France pour créer, comme aux États-Unis, un super-pôle contre-terroriste. Nous avons choisi de maintenir des structures qui avaient chacune leur raison d'être, leur spécialisation, leurs moyens et leurs approches spécifiques. C'est aujourd'hui mon rôle de les amener à exploiter les outils techniques qui ont été développés au service de la communauté.

M. le président Georges Fenech. Je vous ai posé des questions très précises. Ce qui frappe, d'emblée, c'est que tous les individus qui ont commis les attentats, sans exception, étaient connus de nos services. Le problème n'est pas qu'ils aient échappé à leur surveillance à un moment ou à un autre. Je le répète, pourquoi avoir interrompu les écoutes visant les frères Kouachi et Amedy Coulibaly ? Comment Samy Amimour, qui était sous contrôle judiciaire, a-t-il pu quitter le territoire ? Pourquoi n'était-il pas surveillé ? Comment Ismaël Omar Mostefaï, objet d'une fiche S, a-t-il pu quitter lui aussi le territoire ? Comment expliquer que, tout au long de l'année, Abdelhamid Abaaoud ait pu rester hors des radars ? Il faut faire un constat : ils nous ont échappé, on ne peut le nier.

M. Didier Le Bret. Vous avez certainement tous participé, à un titre ou à un autre, à l'élaboration des deux lois de juillet et novembre 2015. Vous savez donc combien les

interceptions de sécurité, pour ne parler que d'elles, sont encadrées. Aux termes de l'article L. 851-2, je le répète, il faut que la menace terroriste soit avérée ; ce dispositif, qui a tant fait parler de lui, ne peut en réalité être appliqué à n'importe qui : il est très sélectif. En outre, la durée d'écoute ou de collecte des données de connexion ne peut excéder deux mois. Cela signifie que, si nous devons exploiter l'ensemble des sélecteurs qui nous intéressent, il nous faudrait demander toutes les dix minutes à la CNCTR de renouveler une autorisation.

Je ne réponds pas à votre question s'agissant de savoir ce qui s'est passé lorsque c'était la Commission nationale de contrôle des interceptions de sécurité (CNCIS) qui décidait du renouvellement des autorisations touchant les interceptions de sécurité ou permettant d'accéder au fichier des personnes que vous avez citées. Mais, vous le savez mieux que personne, l'exécutif suit quasi systématiquement les recommandations de l'autorité administrative indépendante. C'est en tout cas ce qui se passe aujourd'hui.

Bref, les services de renseignement ne « branchent » pas les gens de manière sauvage, mais dans le cadre de procédures triplement encadrées – par la CNCTR, le Conseil d'État et le contrôle parlementaire.

Il y a eu des interruptions, mais celles-ci étaient motivées par le fait que les individus ne semblaient plus particulièrement dangereux à ce moment-là.

Le quota maximal d'interceptions simultanées était fixé à 2 190 en 2014. Même en renouvelant le nombre par tiers, on finit nécessairement par atteindre cette limite.

M. le président Georges Fenech. Cela a donné *Charlie Hebdo* et *l'Hypercacher* !

M. Didier Le Bret. Oui, mais c'est aussi le résultat d'une politique publique assumée par nos autorités et par le Parlement.

M. Christophe Cavard. Voilà plusieurs années que nous réfléchissons aux évolutions du renseignement. Ainsi, la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés, dont Jean-Jacques Urvoas était le rapporteur et moi-même le président, a formulé des préconisations concernant le recrutement. Les chiffres que vous citez s'étendent sur plusieurs années ; nous aimerions savoir ce qui a été fait à ce jour, sachant que le risque s'est hélas accru. Quant aux profils, nous recommandions l'embauche de linguistes et de techniciens, notamment en informatique, car nous avons découvert avec une grande surprise, lors des auditions, l'existence de graves failles techniques qui obligeaient les services à externaliser une partie de ces compétences, ce qui pose évidemment des problèmes s'agissant de renseignement. Ces aspects ont-ils évolué sous l'effet des demandes du Président de la République et des travaux récents ? Nous interrogerons également les directeurs des services à ce sujet.

Ce qui ressort de la réunion du 14 janvier dernier entre le Président de la République et l'ensemble des services de renseignement nous pousse à nous interroger. Il s'agissait d'améliorer la mutualisation et la complémentarité du travail des services. Finalement, selon la presse – parfois mieux informée que les parlementaires –, il n'a pas été décidé grand-chose, sinon que l'on affectera des effectifs sur des terrains où il n'y avait plus personne. C'est du moins ce que j'ai lu dans *Le Monde*. Quel était l'enjeu de cette réunion et que fait-on pour rendre les services de renseignement plus efficaces ?

Enfin, en ce qui concerne les branchements et débranchements, il me semble que l'on était loin, ces dernières années et notamment du temps de la CNCIS, d'atteindre le quota maximal d'écoutes. Les responsables peuvent tout à fait décider de « débrancher », mais cela

ne semble pas pouvoir être pour cette raison. Nous allons aussi interroger le nouveau président de la CNCTR sur ce point. L'autorité exprime des avis, mais c'est l'exécutif qui décide en dernière instance.

M. Alain Marsaud. Monsieur le coordonnateur national, j'ai eu l'occasion de travailler avec vous dans le cadre de vos précédentes fonctions à la tête du centre de crise du Quai d'Orsay, et d'apprécier votre engagement au service de la nation, compte tenu des contraintes de notre politique étrangère.

Le vétéran que je suis constate que, depuis quelque trente ans, au sein du contre-terrorisme, on bricole, on crée des organismes de coordination – j'ai ainsi participé à la création de l'UCLAT, du comité interministériel de lutte antiterroriste (CILAT), du service central de la lutte antiterroriste (SCLAT) –, on connaît des succès, des échecs. Voilà pourquoi je suis très indulgent vis-à-vis des échecs observés autour des attentats de janvier comme de ceux de novembre, et qui concernent les services de renseignement et de sécurité. Naturellement, nous avons à l'esprit le point de vue des victimes et de leurs familles. Mais il ne s'agit pas d'une science exacte et je sais combien il est difficile d'obtenir des résultats en permanence.

Le parcours d'Abaaoud est tout de même extraordinaire : il est dans le viseur des services et se promène un peu partout, du Moyen-Orient à l'Europe.

Mais en ce qui concerne ceux que vous identifiez, que vous interceptez et que vous localisez, existe-t-il une doctrine d'emploi permettant leur élimination préventive – et répressive, quand on sait ce que ces gens ont pu faire et ce dont ils sont capables ? Je vous pose cette question au risque de choquer certains membres de la commission d'enquête ; je la poserai également au patron de la DGSE et à d'autres que nous auditionnerons.

J'étais il y a une semaine à Djibouti, sur la base américaine d'où les drones Predator, armés de missiles Hellfire, décollaient vers le Yémen. Des officiers américains et des agents des services de renseignement, notamment de la CIA, nous ont expliqué que ces drones partaient le soir vers des cibles et qu'ils tuaient – de préférence des Américains, nous a-t-on dit, même s'ils en tuent aussi d'autres. C'est une doctrine d'emploi ; manifestement, au plus haut niveau de l'État – qu'il s'agisse de M. Obama ou de ses collaborateurs –, on décide de faire tuer des gens. Il y a aussi des opérations spéciales dont nous pouvons être informés par nos services, notamment du fait des forces spéciales – qui agissent déjà ainsi, semble-t-il, mais ce sont, dit-on, des actions de guerre.

Ne peut-on envisager de pratiquer l'élimination pure et simple ? J'étais tout récemment avec quelques collègues à Washington, au département de la sécurité intérieure ; les Américains nous ont expliqué que 150 de leurs ressortissants étaient partis en Syrie et, surtout, en Irak, qu'ils ne rentreraient pas puisque trente ans de prison les attendaient à leur retour, et qu'ils allaient tous être « dronés ».

J'ai posé la même question au ministre de la défense.

M. le rapporteur. Mais on le fait déjà !

M. Alain Marsaud. On « drone » ? Le ministre de la défense m'a pourtant répondu que nous n'avons pas de doctrine d'emploi de ce type et que nos drones Reaper n'étaient pas équipés pour mener des actions de guerre. Et on utilise des Rafale. Avec le dronage, on peut cibler un individu, une voiture, etc. Mais cela suppose une doctrine d'emploi : il faut que quelqu'un, au plus haut niveau de l'État français, décide d'éliminer ces gens-là.

Est-ce déjà fait, est-ce faisable ? Pouvons-nous nous donner une telle doctrine ?

M. le président Georges Fenech. Je ne sais si cette question est du ressort de M. Le Bret.

M. Alain Marsaud. C'est le coordonnateur national !

M. Didier Le Bret. En ce qui concerne la doctrine d'emploi, le concept de *high value individual* (individu de grande valeur) vaut pour la France comme pour les États-Unis et pour tous ceux qui sont engagés dans la coalition de lutte contre le terrorisme. Le commandement des opérations spéciales (COS) du ministère de la défense, avec à sa tête le général de Saint-Quentin, pilote par exemple l'opération Sabre, dans le cadre de l'opération Barkhane. Mais cela répond en partie à votre question : nous préférons que ces cibles soient arrêtées vivantes, de manière à les interroger et à enrichir ainsi les informations dont nous disposons. Quand on compare ce que l'on savait de ces gens au début de l'opération Serval, en janvier 2013, et ce que l'on en sait aujourd'hui, on mesure le chemin parcouru.

M. Alain Marsaud. Si on identifiait un Abaaoud aujourd'hui, serait-on en mesure d'agir ?

M. Didier Le Bret. Lorsque le Président donne des instructions sur nos opérations militaires au ministre de la défense ou au chef d'état-major des armées en conseil de défense ou en conseil restreint, il n'est pas question de cibler des individus. On identifie à Raqqa, à Mossoul ou à Deir ez-Zor les états-majors, les centres de propagande, d'entraînement, les dépôts d'armes, bref les lieux stratégiques du point de vue logistique. Ce sont les fameux dossiers d'objectifs. Ce sont eux qui sont ciblés dans le cadre de la guerre que nous menons contre l'État islamique, en Syrie comme en Irak. Si par malheur – ou par bonheur – il se trouve que les individus dont nous parlons s'y trouvent, nous ne revendiquons pas explicitement, surtout s'ils sont français, le fait de les frapper à l'instar des Britanniques ou d'autres. Nous ciblons des objectifs qui font sens afin de réduire la surface occupée par notre ennemi.

M. le rapporteur. J'imagine que vous avez lu le dossier du *Parisien* daté du 13 mai, selon lequel, si nous avons commencé à bombarder la Syrie, c'est parce que nous savions qu'Abaaoud et consorts préparaient des attentats sur notre territoire. Cela tend à contredire votre propos : nous aurions alors précisément ciblé des individus.

M. Didier Le Bret. C'est bien ce que je viens de vous dire.

M. le rapporteur. Vous dites que les cibles sont générales.

M. Didier Le Bret. Vous imaginez bien que ce dont vous parlez est aussi l'effet recherché dès lors que nous avons identifié des lieux de commandement stratégique, des états-majors, des centres de propagande, des endroits où se préparent des attaques dirigées contre notre pays.

La question des peines encourues par les Américains dont a parlé M. Marsaud évoque un enjeu essentiel dont nous avons récemment débattu avec le ministère de la justice : l'évolution de la politique pénale française en vue de criminaliser ce qui relève aujourd'hui du délit.

Pour le dire très clairement, 80 % au moins des personnes actuellement détenues pour des actes de terrorisme vont être libérées au cours des cinq années à venir, soit plus de 70 individus au cours des deux prochaines années. La courbe sera fortement exponentielle puisque près de 300 personnes sont actuellement mises en examen ; or, en l'état actuel de

notre politique pénale, ces gens-là – ceux qui ont préparé les attentats, puisque l'on n'arrête jamais ceux qui les ont commis – encourent des peines maximales de dix ans, sans compter les non-lieux, ce qui revient en pratique à sept ou huit ans, trois ans compte tenu des remises de peine. Bref, des cohortes d'individus qui ont été mis en examen, jugés et détenus vont commencer à sortir de prison au cours des mois qui viennent.

Pour notre sécurité, il est donc essentiel de modifier notre politique pénale afin de ne plus faire de différence entre le crime et le délit, entre le soutien logistique et la participation directe à une action terroriste. Lorsque, dans six mois, vous me demanderez, cette fois à propos de ces anciens détenus, si un suivi continu est possible, ma réponse sera la même : non. Ces individus vont sortir de prison, adopter un comportement très furtif, ils ne se présenteront pas à Pôle emploi, ils ne commettront aucun délit, et aucune obligation de pointer, aucun bracelet électronique ne les empêchera de disparaître quand ils le voudront pour revenir ensuite nous frapper ! La durée de détention et les peines sont un véritable problème.

Monsieur Cavard, en ce qui concerne les moyens, les chiffres que j'ai cités correspondent aux renforts qui ont été déployés par vagues successives, après janvier, au printemps et au moment où le Président en a fait l'annonce devant le Congrès. Sans en détailler la liste par services, en voici le total : en 2016, 1 339 effectifs ; en 2017, 2 228 en cumulé, et 2 617 en 2018. Malheureusement, les directeurs des services vous le diront, il faut un délai de recrutement et de formation avant que ces personnels ne soient opérationnels. Ce qui a été fait depuis deux ou trois ans commence à produire ses effets, mais la montée en puissance est progressive.

Le vrai problème est celui des profils. Jusqu'à une date récente, pour des raisons statutaires, la DGSI n'a pas été en mesure d'opérer la mue fantastique qu'a accomplie la DGSE en s'ouvrant à des administrateurs civils, d'anciens élèves de Sciences Po, des analystes, des ingénieurs, des polytechniciens. La direction technique de la DGSE ne s'est pas constituée en six mois : il a fallu quinze ans d'investissements, d'ouverture, de communication. Mais la DGSE n'a pas de problème de statut : elle peut s'adapter, rémunérer ses agents – car le tout n'est pas de recruter, encore faut-il fidéliser ses cadres, qui ne doivent pas s'évaporer au bout de quelques années après avoir eu accès à des informations sensibles. Cela dit, le fait que la DGSI ait été séparée de la DGPN pour devenir une direction générale lui donne sans doute plus de flexibilité pour recruter des non-titulaires hors du corps des policiers.

Quoi qu'il en soit, les choses suivent leur cours. Patrick Calvar vous le confirmera. Elles ne changeront pas d'un seul coup, comme par magie.

Les décisions prises lors du conseil national du renseignement du 14 janvier sont couvertes par le secret défense et ce qu'en dit *Le Monde* est une extrapolation à partir du communiqué. Dans ce communiqué, on pouvait certes décrypter plusieurs éléments, comme certains journalistes ont tenté de le faire.

D'abord, le *leadership* renforcé de la DGSI en matière d'antiterrorisme. Cette dynamique nouvelle est claire, voulue et assumée.

Ensuite, la mobilisation par l'État des moyens techniques existants, dans le cadre de la loi. Pour le dire clairement, il s'agit de s'assurer que les moyens de la DGSE sont à la disposition de la DGSI, afin de pouvoir soumettre à un travail de discrimination l'environnement sinon des 14 000 signalés, du moins d'une partie d'entre eux, de manière à ce que nous nous concentrons ensuite sur le segment qui nous intéresse.

M. le rapporteur. On a l'impression qu'aujourd'hui, une multiplicité de fichiers coexistent. La DGSI estime que le FSPRT ne lui sert à rien, alors que la gendarmerie et le SCRT le trouvent utile. Les cellules Allat et Hermès ont une liste de noms gérée en temps réel, chacun avec son fichier puisque l'interconnexion n'est pas possible : les représentants de chaque service se réunissent dans une même salle, chacun avec son ordinateur, et font état de leurs informations.

Le haut du spectre est traité par le fichier DGSI. Or celui-ci est la chasse gardée de la DGSI.

M. Didier Le Bret. Non : sauf pour les actions en cours qui peuvent être extrêmement sensibles, notamment parce que les sources doivent être protégées, ce fichier est en interface avec les bases de données utilisées dans le cadre de la cellule Allat.

Quoi qu'il en soit, les services ont une grande habitude de travail opérationnel ensemble. Il ne faut pas s'exagérer leur cloisonnement. Ce travail en commun sert leur intérêt : ainsi, quand un service perd la trace d'un individu qui ne se trouve plus sur le territoire national, il lui faut bien dialoguer avec la DGSE et d'autres services, y compris étrangers, pour le localiser.

M. le rapporteur. En effet, on ne peut pas soupçonner les services de faire de la rétention d'information : l'enjeu est trop important. Mais il est tout de même extraordinaire qu'il faille réunir les représentants des six services dans une salle pour récupérer des informations, au lieu de créer un fichier commun ! Cela vaut du haut du spectre, au sein d'Allat, comme du FSPRT, que la DGSI qualifie de « fichier des préfets » et dont certains services du premier cercle ne connaissaient même pas l'existence quand nous les avons interrogés.

La question des fichiers est donc un enjeu essentiel, qui concerne la mise en commun des bases de données, donc la coordination.

M. Olivier Marleix. En novembre 2015, Bernard Squarcini, ancien patron de la DCRI, révélait qu'il aurait transmis à la France un message des services de renseignement syriens proposant, à condition que nous reprenions contact avec eux, de nous transmettre une liste de djihadistes français présents en Syrie ; cette proposition se serait heurtée à une fin de non-recevoir. Êtes-vous au courant de cette affaire et de la façon dont elle a été traitée ?

La chaîne britannique Sky News dit avoir récupéré une liste de 22 000 Européens ayant rejoint les rangs de l'État islamique. Les services du ministère britannique de l'intérieur et leurs homologues allemands déclarent travailler sur ce document, dont les commentaires publics semblent attester la réalité, même s'il comporte sans doute des redites qui réduisent le nombre de personnes concernées. Les services français ont-ils eu communication de cette liste, et travaillent-ils sur elle ?

M. François Lamy. Je ne vous demanderai pas de confirmer ou non qu'une frappe a visé Abdelhamid Abaaoud le 27 septembre 2015, comme l'affirme l'article du *Parisien* déjà cité. Il semble en tout cas que nous ne nous contentions pas de cibler des centres de décision, mais que nous le faisons pour atteindre quelqu'un en leur sein. Est-ce légal ? Car si le service action de la DGSE est par définition chargé d'actions secrètes qui échappent au cadre légal, ce n'est le cas ni de l'armée de l'air ni, *a fortiori*, du COS, dont les actions sont discrètes, ce qui n'est pas la même chose. Je ne suis pas choqué que l'on agisse ainsi, mais je me demande dans quel cadre juridique on peut le faire. Il ne s'agit même pas de savoir qui doit prendre la décision, mais de protéger ceux qui sont chargés de l'exécuter le cas échéant.

Après le 13 novembre ont été diffusées beaucoup d'informations sur les terroristes et l'on a vu se dessiner sinon des organigrammes, du moins des contacts entre les cellules impliquées dans les différents attentats. Certes, il est toujours facile de reconstituer ces structures après coup. Toujours est-il que les données ne peuvent jouer leur rôle, qui est essentiel, que s'il y a quelqu'un pour les analyser correctement, en comprenant la manière dont ces individus raisonnent, vivent, ont vécu et en en déduisant l'existence de tel ou tel lien.

À votre niveau, avez-vous vu passer ce type d'organigrammes avant les attentats ? Quelqu'un, au sein des services, est-il chargé d'établir ces connexions ? J'ai posé la même question au juge Trévidic. Car nous nous intéressons bien entendu à ce qui s'est passé, mais aussi à la manière de nous protéger à l'avenir. Le nombre de Français partis a atteint au moins un millier, sans parler de ceux qui sont présents sur le territoire ; mais ces organigrammes ne concernent que 120 à 150 personnes. À cet égard, où faites-vous porter vos efforts ? Il ne s'agit plus de mener des recherches tous azimuts, mais d'identifier des connexions permettant de circonscrire la menace une fois pour toutes.

M. Didier Le Bret. En ce qui concerne l'offre supposée des services syriens, je n'ai rien vu de pareil. Comme vous le savez, nous n'avons aucun contact avec ces services. Même dans des domaines plus ordinaires où ils auraient pu nous aider, sans même que nous ayons à le demander, par l'intermédiaire de la Russie ou de la Jordanie, ils ne nous ont jamais fourni le moindre renseignement utile. Je songe par exemple aux séries de passeports vierges récupérés par Daech et sur lesquelles il nous serait très précieux d'avoir des informations. De mon point de vue, tout ce qui a été dit sur la bénévolence et les dispositions à coopérer de M. Mamlouk et de ses affidés est donc dénué de fondement. Quand bien même la situation serait différente, il n'est pas conforme à notre vision des choses, comme vous le savez, de travailler avec un service qui torture et se fait le principal exécuteur des basses œuvres de Bachar al-Assad. Nos services sont tenus de respecter cette injonction politique.

En ce qui concerne Sky News, j'ai interrogé les services à plusieurs reprises ; pour l'instant, et sous bénéfice d'inventaire, je n'ai pas le sentiment que notre capacité à identifier qui que ce soit en ait été révolutionnée.

M. Olivier Marleix. Les services français ont-ils la liste ?

M. Didier Le Bret. Oui, bien sûr. Ils sont en contact avec les Britanniques et nous croisons nos informations. Mais, encore une fois, je ne crois pas que cela ait changé grand-chose à notre connaissance des « stocks ».

Monsieur Lamy, je ne peux que vous répéter ce que je disais tout à l'heure : nous ne revendiquons pas des frappes individuelles, surtout dans le cadre d'une opération militaire officielle. Le fondement juridique est la légitime défense, qui justifie l'action de nos forces armées. Mais nous nous refusons à agir comme les Britanniques, en ciblant précisément des individus.

La reconstitution des organigrammes est l'un des principaux objets du travail de la DGSE, en lien avec les autres services. Ce n'est pas simple, car beaucoup d'acteurs ont des alias multiples, et les choses changent souvent au moment même où nous commençons, grâce à une interception, à nous faire une vague idée de leur identité et de leurs activités. Mais nous savons à peu près qui fait quoi dans les états-majors qui nous intéressent.

M. François Lamy. Depuis quand ?

M. Didier Le Bret. C'est difficile à dire : je vois beaucoup d'organigrammes, mais qui évoluent.

M. François Lamy. Puisque vous en voyez beaucoup, vous pouvez identifier ceux qui sont fondés sur des faits. Cela donne une base de travail, même si certains peuvent se recouper, voire se contredire.

M. Didier Le Bret. Nous avons peu d'informations avérées, étayées sur des fichiers ou des interceptions, concernant les contacts de telle cellule avec tel état-major. En revanche, nous savons quels ont pu être les donneurs d'ordre dans la plupart des attaques.

M. Serge Grouard. En ce qui concerne les bases de données, j'ai la même impression de flou que le rapporteur.

Si un agent de la DGSI veut suivre tel ou tel individu, peut-il aller directement consulter les fichiers de la DGSE, ou doit-il solliciter celle-ci ? Dans cette dernière hypothèse, il ne s'agit pas d'une base de données commune, mais de compatibilité des systèmes. Or j'ai le sentiment que les systèmes ne sont pas compatibles. Qu'en est-il exactement ? Concrètement, les ordinateurs sont-ils compatibles ? Le dispositif a-t-il été conçu dans la perspective d'une gestion commune ? Non ! Or, quand les systèmes informatiques sont différents, il est redoutablement difficile de les rendre compatibles. Vient un moment où il faut changer tous les systèmes techniques. Cette question se pose-t-elle ? Ne veut-on pas le faire ? Existe-t-il d'autres procédures d'échange auxquelles on pourrait recourir ?

Vous disiez tout à l'heure qu'il fallait travailler en temps réel ; cela peut sembler évident, c'est pourtant essentiel. Mais comment faire lorsque les systèmes ne le permettent pas ? Il faut téléphoner, être assuré de joindre son correspondant, qui doit obtenir une autorisation. Tout cela, bien sûr, a été organisé de manière à préserver la sécurité des données, qui ne doivent pas pouvoir être consultées par chacun à son gré. Mais est-ce encore adapté ? Ne faut-il pas accepter de perdre un peu de cette sécurité pour gagner beaucoup en efficacité et en réactivité ?

M. Didier Le Bret. Il est nécessaire de distinguer plusieurs aspects. D'abord l'interconnexion des fichiers, qui est redoutablement complexe et soumise aux contraintes juridiques que vous connaissez et que la Commission nationale de l'informatique et des libertés veille à faire respecter – même s'il existe des fichiers de souveraineté.

Ensuite, au sein des cellules qui ont été citées, les différents services dialoguent directement, en temps réel, à propos de tel ou tel individu qui les intéresse.

Enfin, la plupart de ces services ont des personnels mis à disposition dans les autres services, au niveau des sous-directions, de la direction du renseignement, de la direction technique, de la sous-direction anti-terroriste de la DGSI.

En réalité, donc, les intéressés s'appellent et se parlent en permanence. L'interopérabilité, y compris humaine, existe. Cela ne résout pas entièrement le problème ; mais, nous y travaillons.

Le problème n'est pas seulement l'interopérabilité ou l'interconnexion entre les bases de données des services de renseignement ; il s'agit aussi de s'assurer que les moyens techniques dont disposent nos services peuvent être pleinement exploités par les services d'enquête judiciaire – en Grande-Bretagne, cela ne pose aucune difficulté – et que l'on ne nous oppose plus des obstacles techniques à l'exploitation des données de tel ou tel téléphone. C'est un autre aspect sur lequel nous travaillons beaucoup.

De même, et cela fait partie des quatre-vingts mesures, dont cinquante nouvelles, du plan d'action contre la radicalisation et le terrorisme annoncé il y a peu par le Premier

ministre, nous aidons le service de renseignement pénitentiaire à se doter d'outils et à se mettre à niveau.

M. Serge Grouard. C'est un très bon exemple !

M. Didier Le Bret. Ce faisant, je suis pleinement dans mon rôle d'animation des services. La loi va d'ailleurs – dans les semaines qui viennent, je l'espère – faire du renseignement pénitentiaire un service du deuxième cercle à part entière, ce qui lui permettra d'accéder à certaines techniques et de coopérer davantage avec l'ensemble des services. Cela devrait produire d'importants résultats.

M. le président Georges Fenech. Le rapporteur et moi-même avons rencontré hier M. Calvar, que nous devons auditionner la semaine prochaine. Il estime que l'on ferait un progrès considérable en trouvant une formule juridique permettant de partager l'information judiciarisée, comme le font les Américains. En France, lorsqu'un renseignement est judiciarisé, la DGSI, cosaisie, peut l'utiliser, mais non le communiquer à la DGSE, ce qui pourrait pourtant se révéler précieux, à cause du secret de l'instruction. Cela fait-il l'objet d'une réflexion ?

M. le rapporteur. Confirmez-vous que la DGSI ne peut pas avoir accès au simple fichier STIC (système de traitement des infractions constatées) ?

M. Didier Le Bret. Non : elle y a accès puisqu'elle est à la fois service de renseignement et service de police judiciaire.

M. Meyer Habib. Comment qualifieriez-vous vos liens avec les services étrangers, en particulier américains, britanniques, russes, arabes, israéliens ?

En ce qui concerne l'UCLAT, des gens de la maison, des policiers me disent ne pas bien comprendre son fonctionnement, son classement, etc. Le caractère secret de ces matières crée une sorte de chape de plomb à laquelle ils ont tendance à se résigner. Mais il nous appartient de nous interroger sur ce fonctionnement et sur les possibilités de l'améliorer.

Qu'en est-il de l'utilisation des « taupes », des agents infiltrés, payés pour cela et censés ressembler à tous points de vue aux terroristes ? Beaucoup de services, notamment les services israéliens, que je connais bien, privilégient le renseignement humain.

Cela dit, le domaine technologique connaît des avancées considérables et très rapides. J'ai été récemment approché par des *start-up* qui sont en train de développer de nouveaux systèmes utilisables en milieu pénitentiaire et qu'ils cherchent à vendre, notamment en France. Ces systèmes permettent de cibler le brouillage, de savoir, au mètre près, dans quelle cellule on parle, etc. Une autre entreprise disait être en contact avec les principaux opérateurs téléphoniques aux États-Unis, et stocker ainsi des informations portant non sur une personne ciblée, mais sur tout le monde, en permanence. On peut ainsi savoir où tel ou tel se trouvait un an et demi plus tôt et utiliser cette information si le juge l'autorise. Cela ne sera sans doute jamais envisageable chez nous. Car de telles prouesses technologiques, presque difficiles à croire, ont quelque chose de terrifiant : n'importe lequel d'entre nous peut être fiché vingt-quatre heures sur vingt-quatre par l'intermédiaire de son *smartphone*.

M. Didier Le Bret. En ce qui concerne notre coopération avec les autres services, notre premier partenaire reste, de très loin, les États-Unis. Je me suis rendu sur place à plusieurs reprises, et, lorsqu'il a fallu intensifier notre collaboration, en particulier sur le théâtre du Levant, nous avons signé des instructions spéciales, selon la formule américaine, en vue d'être traités comme l'un des *Five Eyes* : nous bénéficions du même accès aux

informations sensibles, ce qui nous permet de construire ensemble des dossiers d'objectifs dans le cadre de la coalition. Cela a fonctionné ; cette étape a représenté un véritable changement. Les Américains ont pu voir que nous étions des partenaires sérieux et que nous maîtrisons nos techniques.

Quant aux autres services européens, j'ai organisé début février la première rencontre des coordonnateurs européens, afin d'accompagner les actions de nos ministres de l'intérieur, singulièrement à Bernard Cazeneuve, s'agissant du PNR (*Passenger Name Record*), du contrôle des frontières extérieures et internes ou du fichier SIS (système d'information Schengen), en allant aussi loin que possible dans la coopération entre services dans ce domaine de souveraineté qui n'est pas communautarisé. C'est nécessaire, car certains outils à la disposition des pays ne sont pas exploités. J'ai invité Gilles de Kerchove, coordonnateur européen du renseignement, à nous aider à identifier tous les points de blocage. Nous promouvons petit à petit cette orientation avec nos amis européens. Sans faire doublon avec les structures plus opérationnelles de lutte contre le terrorisme au sein des services eux-mêmes, il s'agit d'assurer l'efficacité des décisions actées par les ministres de l'intérieur en conseil « Justice et affaires intérieures » (JAI).

Avec les services des autres pays, notre partenariat est moins soutenu, mais nous dialoguons, naturellement. Le service israélien est un service ami ; les Israéliens sont de très bons analystes de la situation.

M. le rapporteur. Et les Turcs ?

M. Didier Le Bret. Je suis allé voir le patron du MIT pour convaincre les Turcs du fait que nous aider à rapatrier nos *returnees* était une bonne chose, mais qu'il était encore préférable de nous permettre d'obtenir d'eux le maximum d'informations. Jusqu'à cette période, en effet, nous les récupérions un peu « secs » : ils n'ouvraient plus la bouche une fois arrivés en France. Il s'agissait pour nous d'avoir davantage d'éléments, notamment par l'intermédiaire de ce que les Turcs eux-mêmes pouvaient capter, par exemple en mettant la main sur des téléphones. Nous sommes en dialogue avec eux à ce sujet. Il existe des marges de progression, mais nous avons obtenu beaucoup : nous avons un agent de liaison, nous sommes les seuls à bénéficier d'un accompagnement de nos ressortissants d'aéroport à aéroport ; il y a peu de pays avec lesquels la Turquie ait poussé aussi loin la coopération. Nous allons voir les Turcs, nous les écoutons, car il faut travailler avec eux : la Turquie est un partenaire important, bien que compliqué.

M. le président Georges Fenech. Il y a aussi eu la visite du ministre de l'intérieur.

M. Didier Le Bret. Oui, bien sûr.

En ce qui concerne l'UCLAT, la tentation est toujours grande de tout mettre à plat, mais il est difficile d'envisager une énième réforme à un moment où les services sont très sollicités. J'entends les doutes dont certains se sont fait l'écho auprès de vous à ce sujet, monsieur le député ; mais il s'agissait, me semble-t-il, d'une étape en vue de créer du lien, comme l'EMOPT aujourd'hui. Nous ne pouvons pas faire abstraction de notre histoire, dont nous avons hérité l'existence de la préfecture de police, la coexistence des forces de police et de gendarmerie, la présence de services de renseignement au sein de la gendarmerie, de la police et au niveau territorial. Peut-être y aura-t-il un « grand soir » où l'on refondra tout cela pour créer un grand service de lutte contre le terrorisme. Dans le contexte actuel, cela me paraît compliqué.

En ce qui concerne les « taupes », de plus en plus de personnes vont revenir, dont nous espérons qu'elles nous donneront des informations qui permettront des infiltrations. La

protection de nos sources est un autre problème sur lequel nous travaillons. Elle suppose de prendre des mesures exorbitantes du droit commun, pour services rendus à notre pays : exfiltration, changement d'identité, création pour la personne concernée d'un petit commerce à l'autre bout du monde... Or ces mesures sont complexes à prendre en l'état actuel du droit. Il existe des dispositions, mais elles ne sont pas suffisantes. Il faudra donc sans doute apporter une petite modification au code de la sécurité intérieure pour assurer aux sources une véritable protection.

M. Christophe Cavard. S'agissant des rapports entre renseignement et justice, il ressort régulièrement de nos travaux – cette commission d'enquête est la troisième sur le sujet – que le pôle antiterroriste, notamment ses juges d'instruction, se plaint de n'obtenir les informations qu'au compte-gouttes. La question de la judiciarisation continue donc de se poser, notamment eu égard aux principes du droit français, dont le droit à la défense. Des évolutions sont-elles possibles ? Est-il envisageable que la justice soit considérée comme un service d'action à part entière, qui ne se contente pas de réparer ou de condamner ?

Je suis récemment intervenu dans un lycée sur ces questions. La proviseure et les enseignants m'ont alors présenté un jeune homme de seize ans dont ils m'ont dit qu'il faisait l'objet d'une fiche S. Ce qui m'inquiète n'est pas qu'il soit fiché S – il y a certainement une raison à cela –, mais que ce soient la proviseure et l'ensemble de l'équipe enseignante qui me le disent. Certes, l'information doit être partagée, quelle que soit d'ailleurs la dangerosité réelle de ce jeune homme – car nous avons tous bien compris à quoi servent ces fiches. Ce sont les services qui ont prévenu la proviseure. Nous ne sommes pas ici en haut du spectre, plutôt dans le registre des signaux faibles. Nous arrivons justement de Belgique où certains élus locaux montent au créneau à propos du partage d'informations. Si le maire de la commune découvre que le chef d'établissement et les enseignants sont au courant alors que lui ne l'est pas, il risque de mal le prendre !

M. Didier Le Bret. C'est une question délicate. Chacun doit rester dans son rôle : on ne peut pas se faire le substitut ou le bras armé des services dans l'exercice d'un mandat électif ou de fonctions de chef d'établissement. Il y a là un glissement qui n'est pas très sain. Je crois en revanche que ce qui, à long terme, fera la différence, c'est la contribution que chacun d'entre nous, là où il est, sera capable d'apporter. J'ai été frappé par le nombre de personnes qui, depuis janvier et plus encore depuis novembre, viennent nous trouver en nous demandant ce qu'ils peuvent faire. Parmi eux figurent des *start-up* et de grandes entreprises du CAC 40 qui ont développé des logiciels pour détecter des têtes de réseau, qui nous parlent de processus chimiques, etc.

Voilà pourquoi j'ai sollicité il y a plusieurs mois Alain Fuchs, président du CNRS, et Thierry Mandon, secrétaire d'État chargé de l'enseignement supérieur et de la recherche : je suis convaincu que, à long terme, la communauté du renseignement se portera mieux si elle est plus fluide, plus ouverte au monde. Un appel à projets lancé par le secrétaire d'État va permettre d'attribuer 5 000 à 10 000 euros à des chercheurs ; on ne sait pas ce que cela va donner, mais, dans le lot, il y aura certainement quelques projets intéressants. Il est important de s'appuyer non seulement sur nos services qui sont à la manœuvre, sur la justice et sur les administrations compétentes, mais aussi sur ces apports et ceux de la société civile. Un rapport de l'Alliance Athéna a également recensé l'ensemble des productions intellectuelles des dix dernières années sur le sujet : c'est passionnant.

Les services doivent s'appropriier ces informations, pour être au fait de l'état de la recherche et diversifier leurs sources. Aujourd'hui, l'information ouverte, si elle est bien exploitée, représente déjà près de 80 % du résultat. Naturellement, les 20 % qui viennent en

propre des services font la différence. Mais il est fondamental de bien traiter l'information. Voilà pourquoi chaque service se dote de structures d'analyse de l'information ouverte ou du *darknet*.

Au demeurant, il n'y aura jamais de mutualisation entre les services si nous ne prenons pas acte du fait que les nouveaux entrants doivent être formés dans un moule commun, par exemple par l'académie du renseignement. Sans interface avec la recherche, dans le respect du secret des activités, ces personnes risquent la sclérose et ne pourront construire un parcours à long terme. La possibilité de carrières dans le renseignement dépend de notre capacité à organiser la mobilité et la reconnaissance d'équivalences de statut.

Ces questions relèvent de chantiers au long cours qui sont eux aussi importants. Car les résultats que nous pourrions obtenir à moyen terme – prendre Mossoul et Raqqa, entamer les finances de Daech, incarcérer le plus grand nombre possible de personnes présentes sur notre territoire et qui incarnent une menace – ne résoudre pas le problème à long terme.

M. le rapporteur. Si vous pouviez accroître vos prérogatives, en quel sens le feriez-vous ? Quel devrait être selon vous, idéalement, le rôle du coordonnateur français du renseignement ?

J'ai critiqué le nombre déjà élevé de structures existantes, mais il me semble que nous manquons d'un équivalent de l'OCAM belge (Organe de coordination pour l'analyse de la menace). Depuis 1995, le niveau du plan Vigipirate n'a pas été abaissé, car le pouvoir politique ne peut prendre la responsabilité de le faire – on assiste au même phénomène s'agissant de l'état d'urgence, mais c'est un autre débat. Le coordonnateur, qui centralise toutes les informations, ne devrait-il pas formuler des préconisations en la matière ? Cela ne permettrait-il pas de dépolitiser la décision ?

M. Didier Le Bret. Aux États-Unis, deux rapports du Congrès, dont l'un s'appuyait sur près de deux ans de travaux, ont débouché en 2004 sur la création du Director of National Intelligence (DNI), instance de coordination de l'ensemble des services. Il faut dire que les États-Unis en comptaient seize, qui n'étaient pas de petits services et qui avaient chacun étendu leur compétence, de manière quasi entropique, à l'ensemble des champs du renseignement, ce qui créait d'importants problèmes de chevauchement. Vous connaissez les enseignements du 11 septembre : toute l'information était disponible, mais il n'existait pas de passerelle entre les différents services. À l'origine, le DNI comptait une centaine de personnes ; ils sont aujourd'hui plus d'un millier.

Je serais surpris que nous en venions à créer une super-agence de coordination de ce type, même si cela peut faire partie de vos recommandations. L'essentiel est ailleurs. Voici en effet ce qui donne du pouvoir au général Clapper, l'actuel DNI. D'abord, c'est son accès au Président ; or rien n'empêche le CNR de bénéficier de la même prérogative dans le cadre de ses fonctions. Ensuite, c'est sa relation d'information quotidienne au Président, grâce au *brief* qu'il lui délivre tous les matins dans le Bureau ovale ; sous une forme différente, le Président de la République est lui aussi briefé tous les jours. Troisièmement, c'est le DNI qui arbitre les budgets des seize agences : cela lui donne un moyen de pression dans le cas où la CIA ne jouerait pas le jeu, où la NSA ferait de la rétention d'information ou se doterait de services qui dupliqueraient inutilement ceux du FBI ou de la CIA et parasiteraient le système. Or ce moyen de pression, je ne l'ai pas, du fait de notre organisation administrative où le budget est organisé par programme et les chefs de programme sont les ministres et leurs représentants. Je n'en dispose qu'à travers les fonds spéciaux : j'adresse une proposition de répartition au Premier ministre, qui la valide ou non. Mais cela ne représente qu'une partie dérisoire des

budgets des services. Pourtant, le budget pourrait être un formidable levier face à un service qui se refuserait à mutualiser tout ou partie de ses moyens.

Quant à l'organisation, je crois beaucoup à la vertu des plateformes, sur le modèle du GCHQ (*Government Communications Headquarters*) britannique et de ses structures, dont l'équivalent de notre GIC (Groupement interministériel de contrôle) et à l'unité d'analyse : chaque service y délègue des personnes qui travaillent ensemble, non six mois à un an comme au sein d'Allat ou d'Hermès, mais pendant des années. Les cadres y apprennent à œuvrer de concert pour s'approprier les données liées au terrorisme et l'analyse que l'on peut en produire. C'est un système qui a fait ses preuves et qui ouvre des perspectives. Je ne sais si nous ferons de même demain, mais nous ne devrions pas nous interdire d'y réfléchir.

Je ne pense pas que nous soyons moins bons que les Britanniques ou les Américains. Ces derniers ne devraient pas nous donner de leçons, car ils ne sont pas dans la même situation que nous : ils n'ont que deux frontières et s'apparentent pour le reste à une île, où l'on a déjà fait une bonne partie du travail lorsque l'on a contrôlé les arrivées par avion. Pour nous, les choses seront toujours plus compliquées. De même, quelle que soit l'organisation que l'on adopte, les instruments techniques peuvent améliorer la performance globale, mais, comme l'a rappelé M. Marsaud, il est difficile de tout verrouiller dans la vieille Europe : nous aurons toujours des maillons faibles.

En tant que CNR, je suis chargé de mettre de l'huile dans les rouages et d'aider les services, non de pratiquer le *name and shame* (nommer et couvrir de honte) ni de tirer des plans sur la comète ou de monter des Meccano administrativo-politiques qui absorberaient toute l'énergie de services déjà sous pression.

Quant à l'OCAM, je ne crois pas que ce soit une structure très opérationnelle.

M. le rapporteur. Il détermine le niveau de la menace.

M. le président Georges Fenech. Mais la décision reste politique.

M. Didier Le Bret. En ce qui concerne Vigipirate, le rôle apolitique dont vous parliez est joué par le secrétaire général de la défense et de la sécurité nationale (SGDSN). C'est lui qui fait remonter l'ensemble des éléments qui contribuent à l'analyse de la menace. En réalité, il ne vous a pas échappé qu'une évolution est quasiment impossible : la rigidité est totale, puisque la seule question que nous nous posons porte sur le moment où nous allons être frappés de nouveau. Mais, dans l'absolu, vous avez raison : il faut une structure qui objective l'analyse de la menace et qui n'hésite pas à abaisser son niveau lorsque c'est nécessaire.

M. le président Georges Fenech. Nous vous remercions pour cette audition riche d'enseignements.

*

* *

Audition, à huis clos, de M. Francis Delon, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), accompagné de M. Marc Antoine, conseiller auprès du président.

M. le président Georges Fenech. Nous avons le plaisir d'accueillir M. Francis Delon, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), accompagné de M. Marc Antoine, conseiller auprès du président.

Monsieur le président, nous vous remercions d'avoir répondu à la demande d'audition de notre commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015.

Nous poursuivons nos investigations sur le renseignement en nous intéressant maintenant à son contrôle. Je rappelle que la CNCTR, qui, aux termes de la loi sur le renseignement, a succédé à la Commission nationale de contrôle des interceptions de sécurité (CNCIS), veille à ce que les techniques de recueil du renseignement soient mises en œuvre sur le territoire national conformément aux textes et qu'elle donne son avis avant la mise en œuvre de moyens de surveillance par les services de renseignement français.

En raison de la confidentialité des informations que vous êtes susceptibles de nous délivrer, votre audition se déroule à huis clos. Elle n'est donc pas diffusée sur le site internet de l'Assemblée. Néanmoins, et conformément à l'article 6 de l'ordonnance 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, son compte rendu pourra être publié en tout ou partie, si nous en décidons ainsi à l'issue de nos travaux. Je précise que les comptes rendus des auditions qui auront eu lieu à huis clos seront au préalable transmis aux personnes entendues afin de recueillir leurs observations. Celles-ci seront soumises à la commission, qui pourra décider d'en faire état dans son rapport.

Je rappelle que, conformément aux dispositions du même article, « sera punie des peines prévues à l'article 226-13 du code pénal toute personne qui, dans un délai de vingt-cinq ans [...], divulguera ou publiera une information relative aux travaux non publics d'une commission d'enquête, sauf si le rapport publié à la fin des travaux de la commission a fait état de cette information ».

Conformément aux dispositions de l'article 6 précité, je vais vous demander de prêter le serment de dire la vérité, toute la vérité, rien que la vérité.

M. Francis Delon et M. Marc Antoine prêtent serment.

La commission s'intéresse particulièrement à la manière dont sont contrôlées les techniques de renseignement mises à la disposition de nos services.

Après les attentats de janvier et de novembre 2015, avez-vous constaté un afflux des demandes d'autorisation en provenance des services et, parmi ces dernières, quelle part représentent désormais celles liées au terrorisme ?

Quelle proportion d'avis défavorables émettez-vous concernant les demandes liées au terrorisme et pour quels motifs ? Quelle est l'évolution constatée ces dernières semaines ?

La CNCIS avait refusé la prolongation des écoutes des frères Kouachi et d'Amedy Coulibaly en 2013 et 2014. Quels sont les critères qui permettent à la CNCTR de donner un avis favorable ? Comment mieux prendre en compte les individus qui appartiennent au bas du spectre ?

En matière d'interceptions de sécurité, le contingent annuel – 2 700 – est-il suffisant compte tenu du nombre d'individus impliqués dans les filières terroristes ?

Comment vous organisez-vous pour faire face à l'afflux de demandes, notamment en matière de données de connexion ?

Dans quels délais la CNCTR est-elle capable de répondre aux demandes des services ?

Quel premier bilan tirez-vous de l'application des nouvelles techniques introduites par la loi du 24 juillet 2015 relative au renseignement ? Cette loi est-elle pleinement entrée en vigueur ou des décrets d'applications restent-ils à publier ? Combien la liste prévue à l'article L. 851-2 du code de la sécurité intérieure – donc le suivi en réel des individus – comprend-elle de noms ? Où en est l'application de l'article L. 851-3 relatif aux algorithmes ? Les dispositions permettant d'écouter l'entourage sont-elles utilisées par les services ? Comment contrôlez-vous l'usage des techniques décentralisées telles que les *IMSI catchers* (*International Mobile Subscriber Identity*) ou les balises ?

Les services du second cercle se sont-ils pleinement emparés de la possibilité qui leur est offerte d'utiliser les techniques de renseignement ? Combien de demandes ont été formulées par ces services depuis l'apparition du décret ?

Estimez-vous que la CNCTR dispose de moyens suffisants pour remplir sa mission ?

Enfin, comment contrôlez-vous *a posteriori* l'usage des interceptions de sécurité ? Combien de recommandations d'interruption des écoutes ont été adressées à la CNCTR ces derniers mois ?

M. Francis Delon, président de la Commission nationale de contrôle des techniques de renseignement (CNCTR). La Commission nationale de contrôle des techniques de renseignement, vous l'avez indiqué, a été créée récemment, par la loi du 24 juillet 2015 relative au renseignement. Elle a succédé à la CNCIS avec des compétences élargies sur lesquelles je reviendrai.

La mission principale de la CNCTR est de vérifier au quotidien que les techniques de renseignement sollicitées sont conformes à la loi et qu'elles portent au respect de la vie privée une atteinte proportionnée aux menaces invoquées.

La CNCTR comprend neuf membres, dont quatre parlementaires représentants, à parts égales, la majorité et l'opposition. L'un de ces parlementaires est d'ailleurs ici présent en la personne de Pascal Popelin. Trois membres de la commission exercent leurs fonctions à plein-temps – parmi lesquels moi-même, comme la loi m'y oblige. Cette collégialité renforce l'indépendance de la commission, favorise le débat et améliore l'effectivité de son contrôle.

Pour ce qui concerne ses effectifs, la CNCTR, lorsqu'elle s'est installée, le 5 octobre dernier, a repris le personnel de la CNCIS, soit cinq agents. Elle a recruté et s'appuie aujourd'hui sur un secrétariat comptant une douzaine d'agents. Notre objectif est d'atteindre le chiffre de dix-huit équivalents temps plein d'ici à la fin de l'année, afin de faire face aux demandes dont nous sommes saisis et d'assurer les contrôles *a posteriori* que nous devons réaliser. Un budget de fonctionnement un peu inférieur à 400 000 euros est alloué à la commission.

Avant la loi du 24 juillet 2015, seules les demandes d'interception de sécurité et de géolocalisation en temps réel suivaient un processus d'autorisation par le Premier ministre après un avis préalable rendu par la CNCIS. La loi ne précisait pas que cet avis était préalable, mais la pratique avait conduit à ce qu'il le fût. Aujourd'hui – c'est là une grande novation de la loi de 2015 –, toutes les demandes de mise en œuvre sur le territoire national d'une technique de recueil de renseignements sont autorisées par le Premier ministre après avis de la CNCTR.

Reste que la commission n'est compétente qu'en matière de renseignement. Notre activité relève de la police administrative et s'arrête au seuil de la police judiciaire. Quand une affaire est traitée par un juge judiciaire, aucune autorisation de technique de renseignement

n'est donnée. Nous veillons au respect de la distinction entre police administrative et police judiciaire.

Pour ce qui est de son activité, depuis sa mise en place le 3 octobre 2015, la CNCTR a rendu plus de 9 000 avis, compte non tenu des demandes d'accès aux données de connexion que la commission contrôle depuis le 1er février 2016 et sur lesquelles je vais revenir. Le nombre d'avis rendus représente un accroissement supérieur à 50 % du volume de demandes traitées par la CNCIS sur la même durée.

La loi du 24 juillet 2015 a prévu que les techniques de renseignement pouvaient être mises en place pour un certain nombre de finalités – vous les connaissez, je n'y reviendrai donc pas –, parmi lesquelles la prévention du terrorisme.

La loi donne également la liste des techniques de renseignement auxquelles les services peuvent avoir recours, à condition qu'elles soient autorisées par le Premier ministre après avis de la CNCTR. On dénombre une quinzaine de techniques qu'on peut regrouper par catégories.

La première regroupe les interceptions de sécurité – c'est-à-dire le contenu et le contenant – et couvrait le champ de compétence de la CNCIS. Il s'agit de la part la plus importante – mis à part l'accès aux données de connexion – des demandes dont nous sommes saisis. Ces interceptions de sécurité sont réalisées par les opérateurs de téléphonie sur demande du service et sont autorisées par le Premier ministre après avis de la commission. Un intercesseur fait la demande auprès de l'opérateur ; c'est le groupement interministériel de contrôle (GIC). C'est également le GIC qui assure l'accès des services au contenu des communications interceptées au sein de ses centres. Les services ne peuvent avoir un accès direct à ces communications que dans les locaux du GIC.

La loi de juillet 2015 a autorisé l'usage d'une nouvelle technique d'interception du contenu des communications à l'aide d'*IMSI catchers* – grâce auxquels on peut recueillir le contenu des correspondances – permettant d'intercepter les communications. Nous n'avons donné un avis favorable à cette technique qu'en de très rares occasions et pour des motifs d'urgence opérationnelle, notamment en matière de prévention d'actes de terrorisme (crainte de la préparation d'un attentat, d'une prise d'otages,...).

Une deuxième catégorie de techniques concerne l'accès aux données de connexion, à savoir le contenant. Il existe un accès aux données de connexion en temps différé. Depuis le 1er février 2016, c'est la CNCTR qui rend un avis sur ces demandes. Une autre possibilité est donnée par la loi du 24 juillet 2015 : l'accès aux données de connexion en temps réel – mais pour le seul motif de prévention du terrorisme et à l'égard de personnes qui ont été identifiées comme présentant une menace. Cette disposition est également en vigueur depuis le 1er février 2016.

On rattache à l'accès aux données de connexion tout ce qui a trait à la géolocalisation en temps réel, qui permet la localisation d'un téléphone portable et son suivi.

Enfin, on peut accéder à des données de connexion par le biais d'un *IMSI catcher*, mais qui ne s'intéresse qu'aux données de connexion. Il s'agit d'une technique beaucoup plus répandue, notamment en matière de terrorisme.

Le troisième type de technique implique l'accès à un lieu ou à un système informatique, qu'il s'agisse, dans ce dernier cas, du recueil de données informatiques sur un ordinateur, de l'accès à distance au contenu d'une messagerie et, éventuellement, du piégeage d'un ordinateur à distance ou par contact. L'accès à un lieu privé ou à un lieu d'habitation

pour réaliser cette opération nécessite une autorisation spécifique. De même, une telle autorisation est nécessaire pour l'accès à un lieu privé ou d'habitation pour capter des images – vidéo ou photo – ou pour le sonoriser. La loi a prévu que, lorsqu'il y a pénétration dans un lieu d'habitation, la décision est nécessairement prise en formation collégiale par la commission.

Le quatrième type de technique, qui a suscité de nombreux débats à l'occasion de l'examen par le Parlement de ce qui deviendra la loi du 24 juillet 2015, relève de l'article L. 851-3 du code de la sécurité intérieure. C'est ce qu'on appelle l'algorithme qui permet le traitement automatisé des données de connexion d'un grand nombre de personnes, avec pour objectif de déterminer ce qui pourrait justifier une alerte et une surveillance particulière. À l'heure où je vous parle, cette technique n'est pas mise en œuvre. La loi prévoit que la CNCTR se prononce sur l'algorithme et fasse, le cas échéant, des recommandations de modification si elle l'estime nécessaire. À ce stade, nous n'avons été saisis par le Gouvernement d'aucune proposition.

M. Sébastien Pietrasanta, rapporteur. Savez-vous où nous en sommes en la matière ?

M. Francis Delon. C'est plutôt aux services du renseignement qu'il faut poser la question ; nous l'examinerons dès que nous en serons saisis.

M. le président Georges Fenech. Y a-t-il un problème technique ?

M. Francis Delon. Il faut savoir qu'il s'agit d'un outil très complexe et qui ne s'achète pas sur le marché. Il faut par conséquent le fabriquer, ce qui nécessite un peu de temps, et, pour cela, d'utiliser des compétences particulières dont dispose l'État. Le travail se poursuit et, lorsque la demande nous sera soumise, nous l'examinerons avec attention.

Enfin, je mentionnerai la surveillance internationale qui peut avoir un intérêt en matière de lutte contre le terrorisme. Cette surveillance est prévue par la loi du 30 novembre 2015. Le cadre juridique est ici assez différent, puisque la CNCTR n'exerce qu'un contrôle *a posteriori*. Sont utilisés en l'espèce des algorithmes qui analysent des données de connexion.

M. le président Georges Fenech. Disposez-vous de ce type de technique de surveillance sur les théâtres d'opérations extérieures ?

M. Francis Delon. La loi du 24 juillet 2015 s'applique exclusivement sur le territoire national. Ainsi, si la direction du renseignement militaire (DRM) veut appliquer des techniques particulières sur un théâtre extérieur, cela ne relève pas du contrôle *a priori* de la CNCTR, puisque les techniques en question seraient mises en œuvre en dehors du territoire national.

Les services qui ont recours aux techniques de renseignement sont les six formant ce qu'on appelle la communauté du renseignement ou services du premier cercle : la direction générale de la sécurité intérieure (DGSI), la direction générale de la sécurité extérieure (DGSE), la direction de la protection et de la sécurité de la défense (DPSD), la DRM, la direction nationale du renseignement et des enquêtes douanières (DNRED) et TRACFIN (traitement du renseignement et action contre les circuits financiers clandestins).

Un décret du 11 décembre 2015 prévoit qu'un certain nombre d'autres services, dits du second cercle, peuvent avoir accès, pour certaines finalités, à certaines techniques de renseignement. Tous ces services sont placés sous l'autorité du ministre de l'intérieur – ils relèvent de la gendarmerie, de la police nationale, de la préfecture de police de Paris, du

service de police judiciaire ; il s'agit donc de services qui ont une compétence mixte, à la fois judiciaire et administrative, ou de services qui n'agissent que dans le cadre de la police administrative, comme la direction du renseignement de la préfecture de police (DRPP). Les demandes de techniques de renseignement peuvent, pour certains services, concerner le terrorisme.

Dans la pratique, les services du premier cercle, plus aguerris, ont d'emblée fait appel aux nouvelles techniques de renseignement prévues par la loi du 24 juillet 2015, tandis qu'il a fallu attendre le décret du 11 décembre 2015 pour les services du second cercle. La montée en puissance se révélant ici plus lente – faute d'expérience pour mettre en œuvre ces techniques. D'où la mise en place de programmes de formation afin d'assurer l'application des techniques sollicitées dans des conditions raisonnables de sécurité et de légalité.

Le fonctionnement quotidien de la CNCTR s'insère dans la chaîne opérationnelle du renseignement. En effet, si un service de renseignement veut réaliser une opération de renseignement, il revient au chef du service d'en valider la demande. Après quoi celle-ci est transmise au cabinet du ministre de l'intérieur, du ministre de la défense ou du ministre des finances. Si le ministre valide la demande, elle est communiquée à la CNCTR qui se prononce dans un délai très court, que la loi a fixé à vingt-quatre heures.

Le dossier est instruit par l'un des membres du secrétariat de la commission pour être ensuite validé par un membre magistrat, à savoir moi-même ou l'un des trois autres membres magistrats de la CNCTR. Cette procédure concerne environ 95 % des affaires.

M. Meyer Habib. Quel délai s'écoule entre la demande et la validation par le ministre ?

M. Francis Delon. Les délais parisiens sont très courts et leur éventuelle prolongation est imputable au service. Toutefois, entre le moment où l'antenne d'un service, dans une région, demande l'application d'une technique, et le moment de la validation de la demande, il peut s'écouler un délai assez long. À Paris, je l'ai dit, le traitement est très court : nous n'utilisons le plus souvent pas les vingt-quatre heures dont nous disposons. Entre le moment où le ministre reçoit la demande et celui où elle nous est transmise, il s'écoule au maximum quelques heures. Et, entre le moment où nous rendons notre avis et celui où le Premier ministre prend la décision, il s'écoule également quelques heures. Au total, le délai parisien est donc d'environ deux jours, trois au plus.

M. Pascal Popelin. Et, en cas d'urgence, le délai peut être de dix minutes !

M. Francis Delon. En effet, nous pouvons, en cas d'urgence, donner notre avis en moins d'une heure. Cela s'est produit. Nous sommes mobilisables vingt-quatre heures sur vingt-quatre et sept jours sur sept – une permanence est assurée.

Nous faisons tout pour ne pas ralentir inutilement le processus du renseignement. Nous contrôlons que la demande qui nous est formulée est légale et proportionnée. Si elle l'est, nous n'allons pas compromettre une opération par des délais excessifs.

M. le président Georges Fenech. Il y a bien une procédure qui permet, en cas d'extrême urgence, de ne requérir l'avis de la CNCTR qu'*a posteriori* ?

M. Francis Delon. La loi prévoit en effet une procédure d'urgence absolue. Elle n'a été mise en œuvre qu'une seule fois, pour un motif de terrorisme. Nous avons été alertés par le cabinet du Premier ministre, lui-même prévenu par téléphone, d'une menace d'attentat imminent. Le Premier ministre nous a fait savoir qu'il ne souhaitait pas prendre le risque

d'attendre ne serait-ce que trente minutes pour que la commission se prononce – ce qu'elle aurait de toute façon été en mesure de faire –, et qu'il prenait immédiatement la décision. Il s'est trouvé – tant mieux – qu'il s'était agi d'une fausse alerte. Le souhait du Premier ministre a toujours été de passer par la commission. Nous nous sommes organisés pour que le passage par la CNCTR ne soit pas un élément de retard anormal ; aussi statuons-nous dans des délais toujours très brefs.

La loi prévoit en outre deux cas où la demande doit être examinée en formation collégiale : le cas où il s'agit d'autoriser la pénétration dans un lieu d'habitation et celui où la technique, quelle qu'elle soit, concerne une personne exerçant une profession protégée – parlementaire, magistrat, journaliste, avocat... Dans ce dernier cas, c'est même la formation plénière qui est requise.

Nous nous réunissons trois fois par semaine en formation collégiale – ce qui ne doit pas être le cas de beaucoup de commissions –, sans compter les réunions impromptues qu'il faut parfois organiser, en formation plénière, pour examiner un cas de profession protégée.

M. le président Georges Fenech. Est-ce déjà arrivé ?

M. Francis Delon. C'est déjà arrivé.

M. Pascal Popelin. Pour la constitution de son quorum, la formation plénière de la CNCTR, aux termes de la loi, ne nécessite pas la présence de parlementaires, lesquels ont toutefois accédé au souhait du président de faire en sorte qu'à chacune de ces réunions l'un d'eux eu moins soit présent – sauf lors de l'examen des demandes de renouvellement de cas sur lesquels nous nous sommes déjà prononcés.

Pour ce qui concerne la profession de journaliste – l'une de celles, protégées, justifiant que la commission se prononce en formation plénière –, la CNCTR en a une conception extensive, si bien qu'il nous arrive d'examiner le cas d'individus dont la qualité de journaliste est sujette à caution.

M. le rapporteur. Ces cas concernaient-ils davantage l'espionnage que le terrorisme ?

M. Francis Delon. Je ne puis malheureusement pas me montrer plus précis, puisque je suis contraint par le secret de la défense nationale.

Reste que, heureusement, il n'est pas si fréquent que nous ayons à examiner des demandes concernant des individus exerçant des professions protégées. L'esprit de la loi implique que la représentation nationale soit présente au sein des formations plénières. Comme l'a souligné Pascal Popelin, si l'affaire n'est pas nouvelle, s'il s'agit du renouvellement d'un cas sur lequel les parlementaires se sont déjà prononcés, leur présence n'est en effet pas indispensable.

Dans le cas où une réunion collégiale est nécessaire, le délai pour donner un avis est porté à soixante-douze heures. Or, même dans ces circonstances, nous faisons en sorte que les délais soient plus courts et qu'ils ne dépassent pas vingt-quatre heures. Nous attachons donc une très grande importance à la gestion des délais – c'est même l'une des tâches principales du président. La loi a du reste prévu que, si nous ne donnons pas d'avis dans les temps prévus, il est réputé rendu – cela n'est jamais arrivé et nous nous efforcerons qu'il en soit toujours ainsi.

Les demandes d'accès aux données de connexion – recueil de fadettes, identification de numéros – n'étaient pas traitées, auparavant, par la CNCIS, mais par une personnalité

qualifiée, un temps placée auprès du ministre de l'intérieur et qui, depuis le 1er janvier 2015, était placée auprès du Premier ministre. Pour les traiter, nous avons repris les deux collaborateurs de la personnalité qualifiée susmentionnée et chacun des autres chargés de mission de la commission est également sollicité.

M. le président Georges Fenech. Comment exercez-vous le contrôle *a posteriori* ? Selon des critères de légalité ou d'opportunité ?

M. Francis Delon. Lorsque nous autorisons une technique, nous nous disons, dans certains cas, qu'il va falloir la suivre. Ainsi, après avoir donné un avis favorable et après que la technique a été mise en œuvre, nous allons vérifier au sein du service comment cette technique a été appliquée.

Le contrôle *a posteriori* suppose une centralisation des données : ce que nous contrôlons doit rester accessible. C'est l'une de nos premières demandes au Premier ministre. Cette centralisation est déjà acquise pour les interceptions de sécurité, pour les géolocalisations en temps réel, mais pas pour les *IMSI catchers* qui peuvent être utilisés en différents points du territoire. Nous organisons avec les services une centralisation parisienne de ces données ; nous y avons accès au siège des services, sans avoir à nous déplacer en province, ce qui ne nous empêche pas de nous y rendre pour examiner la manière dont les services travaillent à l'échelon régional. Nous travaillons donc sur pièces et sur place.

Il s'agit de dialoguer avec les services qui sont demandeurs d'explications sur la manière dont la loi doit être appliquée. Nous leur faisons donc part de nos attentes et prenons note de leurs difficultés – qui nous conduisent, dans certains cas, à adapter nos jurisprudences.

Les contrôles sont différents selon la technique utilisée : ceux concernant la surveillance internationale ne sont pas les mêmes que ceux exercés sur la mise en œuvre de la pose d'une balise par un service sur le territoire national.

M. le président Georges Fenech. Je mesure l'importance de votre responsabilité, mais la CNCTR n'est pas un service enquêteur, elle est un service administratif de contrôle. Quels sont dès lors les critères objectifs en fonction desquels vous refusez une demande, sans avoir à juger de l'utilité de tel ou tel système de surveillance ? Je rappelle que la CNCIS avait refusé la prolongation des écoutes des frères Kouachi et d'Amedy Coulibaly. Forts de quels critères prenez-vous la responsabilité d'accepter ou de refuser une prolongation ?

M. Francis Delon. La CNCIS a publié un communiqué démentant qu'elle ait jamais refusé la poursuite de la surveillance des frères Kouachi.

M. le président Georges Fenech. Nous l'ignorions !

M. Francis Delon. Ce communiqué a été publié par *Le Figaro*.

Le communiqué de la CNCIS dément l'information donnée initialement par *Le Figaro*. À notre connaissance, il n'y a pas eu du tout d'interruption de la surveillance à la demande de la CNCIS.

M. le président Georges Fenech. D'où est sortie cette affirmation ?

M. le rapporteur. Elle précisait en effet que la surveillance avait été interrompue en août 2014.

M. Pascal Popelin. Indépendamment de ce cas, il faut savoir que nous avons accès, en particulier concernant les interceptions de sécurité, à toutes les productions, c'est-à-dire au contenu des écoutes téléphoniques.

M. Francis Delon. Nous avons en effet accès à tout.

M. Pascal Popelin. Et en direct.

Monsieur le président, vous avez à mon avis employé à mauvais escient le terme d'enquête, dans la mesure où nous intervenons préalablement à celle-ci, dès lors qu'un service estime que l'on doit mettre sur écoute une personne qu'il suspecte et motive les raisons pour lesquelles il sollicite l'autorisation de mettre en œuvre une interception de sécurité. Nous exerçons alors un contrôle technique et juridique permettant de vérifier que la personne à surveiller correspond bien aux critères prévus par la loi. Si c'est le cas, l'autorisation est valable pour quatre mois, délai au terme duquel la demande doit être renouvelée. Entre-temps, on peut espérer que le service aura pu rassembler des éléments de nature à étayer sa demande de renouvellement. Or, comme nous avons accès aux productions, s'il n'y a rien de probant dans les enregistrements, la commission va forcément se poser la question de la pertinence de la poursuite de la surveillance. Il en ira de même si, par ailleurs, les motifs allégués par le service pour solliciter une interception ne se sont pas étoffés au fil du temps.

M. le président Georges Fenech. Vous jugez donc en opportunité, non en légalité.

M. le rapporteur. L'écoute des frères Kouachi n'a rien donné. C'est que les interceptions sont rendues difficiles par le recours de plus en plus fréquent à des techniques de cryptage de la part des personnes suspectes. Votre doctrine a-t-elle évolué en conséquence ? Par ailleurs, avez-vous émis des refus de demandes d'interceptions de sécurité liées au terrorisme ? Si c'est le cas, les services sont-ils revenus à la charge concernant tel ou tel individu au point de vous faire changer d'avis ?

M. Francis Delon. Nous devons nous assurer que la demande entre bien dans le cadre fixé par la loi : correspond-elle à l'une des finalités prévues et l'autorité demanderesse est-elle compétente ? Ensuite, nous devons apprécier la proportionnalité entre l'atteinte à la vie privée portée par la recherche de renseignements et la menace à laquelle il s'agit de faire face. Cela ne signifie pas que nous agissons en opportunité : il revient au Premier ministre de prendre la décision de réaliser la surveillance de telle ou telle personnalité, ce qui relève de l'opportunité politique. Nous-mêmes, nous examinons seulement si la demande est légale.

Nous exerçons par ailleurs un contrôle de subsidiarité prévu par la loi pour l'usage des techniques les plus intrusives : avant d'autoriser la pénétration dans un appartement pour y poser un micro, on s'assure que le service ne peut pas avoir le même renseignement par des techniques moins intrusives.

J'en reviens plus précisément au terrorisme, objet des travaux de votre commission. En 2014, le terrorisme représentait 28 % des demandes d'interception de sécurité traitées par la CNCIS, contre 42 % des dossiers concernant la prévention de la criminalité organisée. Depuis 2015, ces pourcentages se sont inversés : le terrorisme est devenu la première raison de demandes de mise en œuvre de techniques de renseignement, à hauteur de 42 %, tandis que les demandes concernant la criminalité organisée sont passées à 28 %. Ensuite, pour répondre au rapporteur, il nous est arrivé de donner des avis défavorables à telle demande relative au terrorisme, mais c'est rare. Le refus tient le plus souvent à une erreur du service – ce qui peut arriver. Il est par ailleurs arrivé que deux services visent la même cible : dans ce cas, nous prévenons le Premier ministre.

M. le rapporteur. Cela arrive-t-il souvent ?

M. Francis Delon. Non, c'est également très rare.

M. le rapporteur. Mais deux services ne peuvent-ils vouloir surveiller un même individu pour des motifs totalement différents ?

M. Francis Delon. Dans ce cas, il n'y a pas de difficulté, mais, s'il s'agit de la même finalité, nous le signalons au Premier ministre, qui choisira le service qui sera autorisé à surveiller. Nous jouons donc ici, de façon certes marginale, un rôle de coordination.

M. Pascal Popelin. Il faut savoir que la cible n'est pas forcément M. Untel, né à tel endroit et habitant à tel endroit. La cible peut être un numéro de téléphone...

M. Francis Delon. En effet, la cible peut ne pas être identifiée.

Le taux d'avis défavorables est de l'ordre de 1 % en général. Il est inférieur pour les demandes liées au terrorisme.

M. le président Georges Fenech. Motivez-vous vos avis ?

M. Francis Delon. Les avis favorables ne le sont en général pas – sauf quand nous voulons apporter une précision. On peut nous demander une interception de sécurité pour une durée de quatre mois ; or nous pouvons estimer que, dans les circonstances particulières de l'affaire examinée, la durée devrait être plus courte et, dans ce cas, nous expliquons pourquoi. Évidemment, quand l'avis est défavorable, il est motivé.

M. Meyer Habib. Avez-vous déjà donné un avis défavorable à une demande liée au terrorisme ?

M. Francis Delon. C'est arrivé dans quelques cas.

Les demandes que nous examinons ne concernent pas le seul terrorisme islamique.

M. Christophe Cavard. Quelles sont vos relations – à supposer qu'elles existent – avec la DGSE ?

Une grande partie de l'application de la loi du 24 juillet 2015 repose sur vous, puisque vous êtes censés contrôler la destruction des données recueillies. Comment procédez-vous ? Certains services, on s'en souvient, souhaitaient les garder plus longtemps que la loi ne le prévoit – quel est votre sentiment sur la question ?

Enfin, pour ce qui est des *IMSI catchers*, il y a un problème technique de transfert des données, qui pose la question de leur centralisation. En outre, la loi prévoit qu'on peut autoriser l'écoute des personnes les plus proches – on pense au débat portant sur le fait de savoir s'il était utile ou non d'écouter les épouses des frères Kouachi. Vous est-il arrivé d'être saisi d'une demande de surveillance de l'entourage d'une personne suspecte ?

M. Francis Delon. Bien sûr, nous avons des relations avec la DGSE comme avec tous les services de renseignement. Nous dialoguons avec eux en permanence et disposons à cet effet de lignes sécurisées. La DGSE est placée sous deux régimes : le régime domestique, car, contrairement à ce qu'on croit souvent, elle peut mener des opérations sur le territoire français – aussi peut-elle nous soumettre des demandes au titre de la loi du 24 juillet 2015 – ; et le régime qui recouvre l'essentiel de son activité : la surveillance internationale, dans le cadre de la loi de novembre 2015 – dont nous contrôlons le respect *a posteriori*.

Pour ce qui est des destructions de données, vous avez raison de rappeler que notre rôle consiste à veiller à ce que la loi soit appliquée et, notamment, à ce que les délais de conservation des données soient respectés. C'est pourquoi j'ai évoqué la nécessité d'une centralisation nous permettant d'avoir accès à toutes les données et de nous assurer que les

délais légaux sont respectés. Ainsi, pour les *IMSI catchers*, qui interceptent les données de connexion, la loi a prévu que, à l'issue d'un délai de quatre-vingt-dix jours au maximum, le service doit avoir détruit toutes les données qui ne concernent pas directement la cible, ce qui suppose un tri entre de nombreux numéros. Nous y veillons et c'est pourquoi nous avons effectué plusieurs contrôles sur cette technique.

Enfin, en ce qui concerne l'entourage des personnes surveillées, la loi prévoit que, en matière d'interceptions de sécurité, peuvent être autorisées des mesures d'écoute sur des personnes qui ne sont pas directement impliquées, mais qui ont une relation étroite avec une cible et avec laquelle cette cible va communiquer – c'est, par exemple, la mère qui appelle son fils en Syrie. La CNCIS considérait qu'on ne pouvait pas autoriser de telles écoutes. La loi l'autorise désormais et nous appliquons donc la loi : nous avons bien sûr autorisé des interceptions de sécurité au titre de l'entourage.

M. le président Georges Fenech. Pourquoi estimez-vous faire partie de la chaîne opérationnelle du renseignement, alors que la CNCTR est un organisme d'autorisation et de contrôle ?

M. Francis Delon. Nous nous situons dans la chaîne opérationnelle parce que nous sommes l'organisme de contrôle qui intervient avant que la décision ne soit prise par le Premier ministre. Et c'est notre avis qui va avoir une grande influence sur cette décision. Jusqu'à présent, le Premier ministre a toujours suivi nos avis défavorables, ce qui n'était pas le cas avec la CNCIS. J'ajoute que, s'il ne suivait pas notre avis défavorable, nous pourrions saisir le Conseil d'État pour contester la décision – ce que ne pouvait faire la CNCIS.

M. le président Georges Fenech. Est-ce déjà arrivé ?

M. Francis Delon. Non. Le Premier ministre ayant toujours suivi nos avis défavorables, la question ne s'est pas posée.

Présidence de M. Meyer Habib, vice-président.

M. Serge Grouard. Comment contrôlez-vous concrètement la destruction des données ? Opérez-vous à partir des données elles-mêmes, de leur contenu, afin de vérifier que la partie qui n'aurait pas trait au domaine couvert par l'autorisation a bien été détruite ?

Ensuite, comment appréciez-vous une demande de renouvellement ? Le service demandeur va-t-il vous communiquer des informations qu'il aura pu recueillir ? Est-ce à partir de là que vous jugez de l'opportunité du renouvellement ?

M. Francis Delon. Pour contrôler la destruction des données, il faut qu'elles soient « traçables ». S'il s'agit d'une interception de sécurité, c'est très facile, car la centralisation est réalisée par le GIC qui s'assure, sous notre contrôle, que les données sont conservées pendant la durée légale. C'est plus compliqué pour les opérations décentralisées. Il faut ici construire un système de centralisation des données qui n'existe pas. C'est compliqué, parce qu'on ne peut transporter les données que dans des conditions qui préservent le secret de la défense nationale. On a par conséquent le choix entre les valises accompagnées, si je puis dire, ou des réseaux sécurisés qui n'existent pas toujours et qu'il faut bâtir. Les données nous parviennent donc soit de manière électronique, soit de manière physique et elles sont étiquetées afin d'être rattachées à telle ou telle opération. Nous vérifions ensuite, si nous effectuons un contrôle dans le service concerné, que la donnée n'a pas été conservée au-delà de la durée légale. Nous opérons au cas par cas selon la technique utilisée.

Il faut avoir présent à l'esprit que nous ne pouvons pas contrôler *a posteriori* la mise en œuvre de toutes les techniques. Nous procédons par sondage, par échantillonnage. Pour tout contrôler, il faudrait des moyens considérables.

M. Pascal Popelin. Le pourcentage d'aléas n'est pas le même selon les techniques.

M. Francis Delon. Nous faisons en effet des choix. Lorsque nous autorisons une technique, si elle nous paraît particulière, nous décidons de la contrôler.

Pour ce qui est du renouvellement, tout dépend, ici aussi, de la technique employée. S'il s'agit d'interceptions de sécurité, nous avons accès à tout moment, dans nos locaux, à l'intégralité des conversations interceptées. Quand une demande de renouvellement nous est soumise, nous allons donc vérifier ce qu'a donné la précédente autorisation. Si les résultats sont en lien avec la finalité invoquée, si le service, qui doit motiver sa demande, nous explique que le renouvellement est nécessaire pour la bonne réussite de l'opération en cours, si nous sommes convaincus par les résultats obtenus, nous répondrons par l'affirmative. En cas de doute, il va falloir porter une appréciation qui varie selon les finalités.

M. Christophe Cavard. Vous avez indiqué précédemment que le taux de demandes d'interceptions concernant le terrorisme était passé de 28 % à 42 % depuis le début de 2014. Qu'en est-il des quotas ? Je crois savoir que l'on n'avait jamais atteint celui fixé par la loi concernant les interceptions de sécurité.

M. le rapporteur. Une liste est prévue par l'article L. 851-2 du code de la sécurité intérieure, concernant le suivi en temps réel d'individus. Pouvez-vous nous en dire un mot ?

M. Francis Delon. Il existe deux quotas, l'un, connu, pour les interceptions de sécurité, qui est de 2 700, l'autre, qui n'est pas public, pour les utilisations simultanées d'*IMSI catchers*, beaucoup plus bas pour des raisons évidentes. Aucun de ces deux quotas n'a été à aucun moment atteint ni même approché. Le quota concernant les interceptions de sécurité est suffisant. Il faut tenir compte de la capacité des services : on aura beau mettre en œuvre des interceptions de sécurité, encore faut-il pouvoir disposer d'analystes pour les exploiter. Bref, ces quotas ne sont pas du tout un frein à l'action des services.

J'en viens à la question sur l'article L. 851-2 du code de la sécurité intérieure. Ce dispositif permet de recueillir en temps réel les données de connexion d'une personne suspectée de représenter une menace en matière de terrorisme – et de terrorisme uniquement. Il s'agit, en pratique, d'effectuer une surveillance à bas bruit d'une personne qui ne justifie pas une surveillance plus poussée – de type interception de sécurité ou autre –, mais qui peut présenter un risque, par exemple parce qu'elle se serait radicalisée. La loi prévoit ici que les autorisations permettent de recueillir non pas le contenu des conversations, comme c'est le cas pour les interceptions de sécurité, mais les données de connexion : qui cette personne appelle-t-elle ? Par qui est-elle contactée ? À quel endroit se déplace-t-elle ? Quel site consulte-t-elle sur internet ? Cette technique commence à être mise en œuvre, mais, pour l'heure, sur un nombre assez réduit de personnes.

M. le rapporteur. Que je comprenne bien : s'agit-il des fadettes ?

M. Francis Delon. C'est cela : on sait qui la personne surveillée appelle, qui l'appelle, où elle se promène sur internet...

M. le rapporteur. Le service demandeur, quand il s'agit de terrorisme, est donc forcément la DGSIS ?

M. Francis Delon. Pas seulement. Cette technique est ouverte à plusieurs services.

M. le rapporteur. Mais il doit s'agir pour 90 % des cas de la DGSI ?

M. Francis Delon. La DPSD est elle aussi concernée par la lutte antiterroriste – notamment dans le milieu militaire –, la DGSE également ou encore la DNRED qui peut apporter sa contribution. Reste que, vous avez raison, les demandes proviennent essentiellement de la DGSI.

M. le rapporteur. Il est ici question des « signaux faibles ». Si je comprends bien, vous vérifiez le degré de radicalité d'un individu. Combien des personnes figurant sur cette liste ont fait l'objet, par la suite, d'une interception de sécurité ? Comment décide-t-on de passer d'une surveillance à bas bruit à une interception de sécurité ?

M. Francis Delon. Je puis vous donner ma vision des choses, sachant que le dispositif est en train de se mettre en place et que des ajustements sont encore nécessaires. La surveillance à bas bruit permet le déclenchement éventuel d'alertes. Dès lors que cette dernière est déclenchée, le service demandeur décide éventuellement d'aller plus loin dans la surveillance.

M. le rapporteur. Pourquoi nos 10 500 fichés S liés à l'islam radical ne sont-ils pas soumis à cette surveillance à bas bruit ?

M. Francis Delon. Il faut poser la question aux services. Je rappelle que l'article 851-2 du code de la sécurité intérieure s'applique à des personnes qui représentent une menace en matière de terrorisme. On est donc au-delà d'une simple suspicion. Il faut un minimum d'éléments tangibles pour la mise en œuvre de cette technique – c'est ce qu'a prévu le législateur.

M. le rapporteur. Pouvez-vous nous donner un ou deux exemples ? Qu'est-ce qu'une menace tangible justifiant une surveillance à bas bruit ?

M. Francis Delon. Est concerné un individu, par exemple, qui, sans être lié à Daech, s'est radicalisé, tient des propos manifestant une empathie à l'égard de mouvements terroristes ou qui peut avoir un comportement qui inquiète. Reste que l'on en juge au cas par cas.

Lorsque nous avons été saisis de demandes par les services, nous les avons examinées chacune avec attention et en avons autorisé une bonne partie ; nous sommes toutefois loin des chiffres que vous indiquez...

M. le rapporteur. Je me demande simplement pourquoi, en matière de surveillance à bas bruit, on ne pêche pas plus large, si vous me passez l'expression.

M. Francis Delon. Parce que la loi ne le permet pas. La loi dispose expressément que l'individu considéré doit représenter une menace.

M. le rapporteur. Toute l'ambiguïté est là. Aujourd'hui 14 000 personnes figurent dans le fichier FSPRT (fichier de traitement des signalés pour la prévention et la radicalisation à caractère terroriste).

M. Pascal Popelin. Il tient compte de tous ceux qui ne sont pas sur le territoire national.

M. le rapporteur. Soit, enlevons-en donc 2 000.

M. le rapporteur. De nouvelles données alimentent régulièrement le FSPRT. Pourquoi les pratiques évoquées ne sont-elles pas couplées ?

M. Francis Delon. Ma réponse est très simple : nous examinerons toutes les demandes que les services formulent.

M. le rapporteur. Les demandes sur ce sujet sont-elles en augmentation ?

M. Francis Delon. Nous en sommes aux débuts de la mise en œuvre de cette technique qui est pointue.

M. le rapporteur. Les services ont-ils pris la mesure de cette technique ?

M. Francis Delon. Ils recueillent des données de connexion, qui sont illisibles pour des personnes non initiées au maniement de l'informatique. Il faut donc des techniciens capables de les exploiter. Cette technique commence à être mise en œuvre sur un périmètre beaucoup plus étroit que celui que vous évoquez. Reste que, si nous sommes saisis de demandes s'inscrivant dans un périmètre plus large, nous les examinerons bien sûr.

M. Meyer Habib, président. Merci, monsieur le président, pour toutes ces précisions et pour la clarté de vos propos.

La séance est levée à 19 heures 15.

Membres présents ou excusés

Présents. - M. Pierre Aylagas, M. Christophe Cavard, M. David Comet, Mme Marianne Dubois, Mme Françoise Dumas, M. Georges Fenech, M. Serge Grouard, M. Meyer Habib, M. François Lamy, M. Jean-Luc Laurent, M. Olivier Marleix, M. Jean-René Marsac, M. Alain Marsaud, M. Sébastien Pietrasanta, M. Pascal Popelin, Mme Julie Sommaruga, M. Jean-Michel Villaumé

Excusés. - M. Jean-Jacques Cottel, M. Jacques Cresta, Mme Lucette Lousteau