

A S S E M B L É E      N A T I O N A L E

X I V <sup>e</sup>      L É G I S L A T U R E

# Compte rendu

## **Commission des lois constitutionnelles, de la législation et de l'administration générale de la République**

- Audition de M. Patrick Calvar, directeur central du renseignement intérieur..... 2
- Informations relatives à la Commission ..... 13

Mercredi

30 octobre 2013

Séance de 10 heures 30

Compte rendu n° 10

SESSION ORDINAIRE DE 2013-2014

**Présidence  
de M. Jean-Jacques  
Urvoas,  
*Président***



*La séance est ouverte à 10 heures 15.*

*Présidence de M. Jean-Jacques Urvoas, président.*

*La Commission procède à l'audition de M. Patrick Calvar, directeur central du renseignement intérieur.*

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

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

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

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

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

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

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

Je voudrais, en quelques mots, vous présenter le travail réalisé par la direction centrale du renseignement intérieur (DCRI) ainsi que les objectifs poursuivis par la création à venir d'une direction générale de la sécurité intérieure. La question sous-jacente est bien celle de savoir si notre pays veut se donner les moyens de se doter d'un service du renseignement intérieur digne de ce nom.

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

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

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

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

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

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

Les méthodes de travail évoluant et les menaces changeant de forme, la DCRI doit disposer des moyens nécessaires à l'accomplissement de ses missions. En contrepartie, son action doit s'inscrire dans un système bien défini d'autorisation en amont et de contrôle efficace en aval pour assurer le respect de la légalité. Pour reprendre l'exemple de l'affaire « Snowden », les fonctionnaires américains ont agi en toute légalité au regard du droit américain et aucun d'eux ne sera poursuivi.

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

**M. Patrice Verchère, rapporteur pour avis.** – Monsieur le directeur central – et peut-être directeur général à partir du 1<sup>er</sup> janvier prochain...

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

**M. Patrice Verchère, rapporteur pour avis.** – Je me réjouis du succès du rapport d'information que Jean-Jacques Urvoas – probablement le meilleur spécialiste des questions liées au renseignement au sein de notre Assemblée – et moi-même avons publié et dans lequel

nous préconisons une évolution de la direction centrale du renseignement intérieur en une direction générale autonome.

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

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

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

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

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

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

Même dans un autre contexte, celui de nos activités judiciaires, nous menons actuellement des discussions au sujet de la protection de l'anonymat des agents qui agissent dans le cadre de procédures judiciaires afin d'éviter qu'ils soient identifiés et que leur nom

soit publié sur des sites Internet, notamment islamistes, avec tous les risques physiques qui peuvent en découler pour leur personne.

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

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

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

Ensuite, bien des agents des services de renseignement sont peu habitués à être auditionnés par des parlementaires. Si, toutefois, on permettait à la délégation parlementaire au renseignement d'entendre tout agent de ces services, il faudrait envisager une limite : le directeur de service doit pouvoir venir accompagné de la personne considérée comme la plus qualifiée. Néanmoins, cette précaution n'exclut pas le risque que désormais, tout agent s'auto-inhibe dans son activité quotidienne, ayant conscience qu'il pourrait être un jour auditionné par la délégation parlementaire. Les agents risquent de voir dans cette nouvelle prérogative de la délégation parlementaire un système de contrôle de plus en plus aigu de leur activité, sans pour autant qu'on leur dise clairement dans le même temps ce qu'ils peuvent ou ne peuvent pas faire.

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

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

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

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

délégation parlementaire puisse être accompagné par la personne la plus qualifiée pour répondre à un point précis avec la plus grande efficacité et en toute transparence.

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

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

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

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

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

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

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

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

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

**M. Yann Galut.** J'ai conscience que la lutte contre le terrorisme et les cyber-attaques constitue, pour vos services, des priorités que, d'ailleurs, nous partageons. Cependant, vous

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

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

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

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

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

**Mme Marie-Françoise Bechtel.** Sur la question de la lutte contre la fraude fiscale, il me semblerait préjudiciable, dans le monde dangereux qui est le nôtre, de confier à un même service des missions d'une telle diversité. Monsieur le directeur central, je partage par ailleurs votre point de vue concernant l'audition éventuelle de vos agents par la délégation parlementaire au renseignement. Il ne faut pas que de telles auditions conduisent à des informations tronquées et ce qu'on peut qualifier de « centralisation du dialogue » au travers des chefs des services me paraît nécessaire.

Je souhaiterais vous soumettre deux questions. D'une part, à l'occasion de l'examen du projet de loi relatif à la sécurité et à la lutte contre le terrorisme, en 2012, nous nous étions interrogés sur l'opportunité d'autoriser l'espionnage actif des réseaux informatiques, c'est-à-dire le fait, pour un agent, de pénétrer un réseau et d'engager un dialogue avec les terroristes

qui y participent. Pour des raisons constitutionnelles, nous n'avions pas examiné ces dispositions. Pensez-vous qu'il soit nécessaire de donner ce pouvoir aux services de renseignement ?

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

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

S'agissant des dérives que vous évoquiez, relatives à l'utilisation des moyens de surveillance d'Internet aux fins d'intelligence économique, je crois que notre pays n'a pas assez pris conscience des dangers que représente l'Internet. Les pouvoirs publics doivent mener une réflexion d'ensemble sur cette question, en s'appuyant sur les organismes existants afin d'inciter les entreprises françaises à engager des démarches d'autoprotection. La sécurité n'est pas une chose naturelle chez nos compatriotes. Nos entreprises n'ont pas la culture qu'ont les entreprises anglo-saxonnes en la matière. Or, la révolution numérique nous montre à quel point le danger est à nos portes, et même a franchi nos portes. C'est un des enjeux majeurs de demain. Nous souhaitons nous doter d'une capacité de lutte, mais cette capacité ne sera pas suffisante, donc il faut, dans le cadre de la communauté du renseignement, que nos services s'intègrent à d'autres, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il faut aller plus loin, au travers de l'éducation, pour modifier les comportements, dans une logique sécuritaire.

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



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

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

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

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

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

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

cadre sur le renseignement qu'appelait de ses vœux votre prédécesseur dans une interview récente ?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

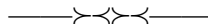
**M. Patrick Calvar, directeur central du renseignement intérieur.** La coopération se poursuit en matière de lutte contre le terrorisme, mais la question peut se poser sur d'autres sujets.

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

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



*La séance est levée à 11 heures 30.*



### **Informations relatives à la Commission**

La Commission a désigné :

*M. Christian Assaf*, rapporteur sur la proposition de loi organique, adoptée par le Sénat, relative à la nomination du président de l’Autorité de régulation des jeux en ligne (n° 1425) ;

*M. Dominique Raimbourg*, rapporteur sur le projet de loi relatif à la prévention de la récidive et à l’individualisation des peines (n° 1413) ;

*Mme Axelle Lemaire*, rapporteure sur la proposition de loi, adoptée par le Sénat, tendant à modifier l’article 698-11 du code de procédure pénale relatif à la compétence territoriale du juge français concernant les infractions visées par le statut de la Cour pénale internationale (n° 741).

## **Membres présents ou excusés**

Présents. - M. Christian Assaf, Mme Marie-Françoise Bechtel, M. Erwann Binet, M. Jean-Pierre Blazy, M. Dominique Bussereau, Mme Colette Capdevielle, Mme Marie-Anne Chapdelaine, M. Jean-Michel Clément, M. Gilbert Collard, Mme Pascale Crozon, M. Carlos Da Silva, M. Jean-Pierre Decool, M. Sébastien Denaja, Mme Françoise Descamps-Crosnier, M. René Dosière, M. Olivier Dussopt, M. Matthias Fekl, M. Georges Fenech, M. Yann Galut, M. Guy Geoffroy, M. Bernard Gérard, M. Yves Goasdoué, M. Philippe Gosselin, M. Philippe Goujon, Mme Françoise Guégot, M. Philippe Houillon, M. Armand Jung, Mme Nathalie Kosciusko-Morizet, M. Guillaume Larrivé, M. Jean-Yves Le Bouillonec, Mme Anne-Yvonne Le Dain, M. Bernard Lesterlin, M. Paul Molac, M. Pierre Morel-A-L'Huissier, Mme Nathalie Nieson, M. Edouard Philippe, Mme Elisabeth Pochon, M. Jean-Frédéric Poisson, M. Pascal Popelin, M. Dominique Raimbourg, M. François Sauvadet, M. Alain Tourret, Mme Cécile Untermaier, M. Jean-Jacques Urvoas, M. Daniel Vaillant, M. Jacques Valax, M. François Vannson, M. Patrice Verchère, M. Jean-Luc Warsmann, Mme Marie-Jo Zimmermann, M. Michel Zumkeller

Excusés. - M. Jacques Bompard, M. Marcel Bonnot, M. Sergio Coronado, M. Marc-Philippe Daubresse, M. Patrick Devedjian, M. Marc Dolez, Mme Laurence Dumont, M. Daniel Gibbes, Mme Marietta Karamanli, Mme Axelle Lemaire, M. Alfred Marie-Jeanne, M. Bernard Roman, M. Roger-Gérard Schwartzberg

Assistait également à la réunion. - M. Michel Ménard