ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Mercredi
18 septembre 2013
Séance de 10 heures

Compte rendu n° 95

SESSION EXTRAORDINAIRE DE **2012-2013**

Compte rendu

Commission de la défense nationale et des forces armées

Présidence
de Mme Patricia Adam,
présidente

ASSEMBLÉE NATIONALE

La séance est ouverte à dix heures quinze.

Mme la présidente Patricia Adam. Je suis heureuse d'accueillir Francis Delon, secrétaire général de la défense et de la sécurité nationale, sur le projet de loi de programmation militaire (LPM).

Je rappelle que le projet de LPM 2014-2019 comporte beaucoup d'avancées sur le plan législatif, notamment sur les services de renseignement et l'accès à de nouveaux fichiers.

M. Francis Delon, secrétaire général de la défense et de la sécurité nationale. Je tiens à vous remercier de me convier devant vous, pour vous apporter des précisions sur certains sujets abordés dans la loi de programmation militaire. Au regard des compétences du secrétariat général de la défense et de la sécurité nationale (SGDSN) et des auditions que votre commission a déjà programmées, il me semble opportun, sauf objection de votre part, de concentrer mon propos sur la sécurité des systèmes d'information, le renseignement et la création d'une plateforme de traitement des données PNR (*passenger name record*).

S'agissant de la sécurité des systèmes d'information, vous savez, madame la présidente, ainsi que MM. Christophe Guilloteau et Edouardo Rihan Cypel, qui étaient membres comme vous de la commission du Livre blanc, combien ce sujet nous a occupés lors des travaux menés par celle-ci. Les dispositions que je vais vous présenter reprennent pour l'essentiel celles que vous avait exposées en juillet Patrick Pailloux, le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Au préalable, je souhaite vous rappeler en quelques mots les cybermenaces auxquelles nous sommes confrontés.

L'espionnage tout d'abord. La situation que nous observons est préoccupante. L'espionnage, souvent d'origine étatique, est massif. En matière industrielle, il atteint tous nos secteurs de souveraineté. Or ce n'est qu'une fois l'attaque réussie et le pillage accompli que les entreprises victimes comprennent la nécessité de renforcer la sécurité de leurs systèmes d'information. Nous ne voulons pas attendre que nos entreprises soient confrontées à ce pillage pour qu'elles réagissent : d'où le choix du Gouvernement de proposer au Parlement des mesures appropriées. Les efforts déployés doivent aussi contribuer à protéger la compétitivité de nos entreprises nationales.

Le deuxième objectif possible pour un attaquant est la déstabilisation. L'attaque est alors médiatisée. Il s'agit de messages de propagande ou d'hostilité placés sur des sites Internet mal protégés à l'occasion d'un conflit, armé ou non, ou bien même d'une décision politique qui suscite la controverse. On se souvient par exemple du *blackout* de l'Internet en Estonie en 2007, qui a privé ce pays de l'accès aux services bancaires et à l'administration en ligne.

Troisième objectif possible : le sabotage. L'attaquant cherche alors à perturber le fonctionnement d'installations connectées aux réseaux de communications électroniques – ce peut être un service bancaire, un château d'eau de l'une de nos communes ou une centrale de production d'énergie. L'exemple le plus frappant nous est donné par le ver informatique Stuxnet qui a perturbé le fonctionnement des centrifugeuses de la centrale de Natanz, détruisant un millier d'entre elles et retardant ainsi le programme nucléaire iranien.

Les précisions sur le cyberespionnage figurant dans le rapport de la société de sécurité informatique américaine *Mandiant* confirment le caractère méthodique d'un pillage systématique effectué à distance par des unités militaires – je rappelle que ce rapport faisait

état d'attaques chinoises. Depuis quelques mois, les révélations quasiment quotidiennes issues des documents de l'ex-consultant en sécurité de la *National Security Agency* (NSA) Edward Snowden montrent l'ampleur de l'espionnage et les moyens considérables qui y sont alloués.

Si les protestations diplomatiques et politiques sont indispensables et pleinement justifiées, elles ne sont pas suffisantes pour nous protéger. Il est urgent de renforcer de manière significative la sécurité des systèmes d'information de nos opérateurs les plus importants.

Les dispositions proposées dans le chapitre III du projet de loi ont deux objectifs.

Le premier est politique. Il est l'affirmation de la nature interministérielle et stratégique de la sécurité et de la défense des systèmes d'information. Le Livre blanc a placé les cyberattaques parmi les menaces majeures auxquelles nous sommes exposés. Et à travers l'ANSSI qui m'est rattachée, je suis témoin, au quotidien, de la réalité de cette menace qui vise et touche tant le Gouvernement et les administrations que les entreprises. Il s'agit ici de donner un signe à tous les acteurs concernés, y compris à ceux qui nous attaquent, de notre volonté collective de faire face à cette menace en adaptant notre droit, notre organisation et nos moyens.

Le second objectif découle du premier. Il s'agit d'accroître de manière sensible le niveau de sécurité des systèmes d'information les plus critiques pour la nation.

J'en viens aux détails des dispositions qui vous sont proposées.

L'article 14 du projet de loi insère deux articles dans le chapitre consacré à la sécurité des systèmes d'information du code de la défense. Il précise les responsabilités du Premier ministre, qui a la charge de la définition de la politique en matière de défense et de sécurité des systèmes d'information et coordonne à ce titre l'action gouvernementale. Il dispose de l'ANSSI pour l'assister dans cette mission ; cette agence est chargée 24 heures sur 24 de prévenir et de réagir aux attaques contre nos infrastructures les plus importantes. Comme elle est rattachée au SGDSN, son domaine d'intervention, initialement centré sur les administrations et les organismes dépendant de l'État, s'est rapidement élargi aux opérateurs d'importance vitale (OIV) et aux entreprises indispensables à notre stratégie de sécurité nationale.

L'article 14 a aussi une vocation opérationnelle et politique.

Opérationnelle : il s'agit de mettre un terme à la situation actuelle dans laquelle l'attaquant a tous les droits et ceux qui sont chargés de la défense, à peu près aucun. L'attaquant a généralement l'avantage sur le défenseur. Les agents de l'État chargés de la sécurité et de la défense des systèmes d'information doivent être en mesure d'utiliser toutes leurs capacités pour mieux appréhender la nature et l'ampleur d'une attaque, en prévenir et en atténuer les effets ou la faire cesser lorsque les circonstances l'exigent.

Il est arrivé que, dans le cadre du traitement d'une attaque informatique en cours contre un fleuron de notre industrie, les ingénieurs de l'ANSSI soient en mesure de collecter des informations susceptibles d'anticiper les mouvements de l'attaquant. Ils auraient dû, pour cela, accéder au système d'information utilisé par celui-ci. Mais ils ne l'ont pas fait car cette intrusion aurait été illégale. Dans l'état de notre législation, les agents de l'ANSSI, comme ceux du ministère de la Défense ou d'autres administrations de l'État compétentes, ne sont pas autorisés par la loi à effectuer toutes les opérations techniques qui leur permettraient d'être pleinement efficaces dans leurs actions. Ainsi, le code pénal prohibe de manière générale la pénétration de systèmes de traitement automatisé de données. Le projet de loi vise donc à

rétablir une forme d'équilibre en permettant au défenseur d'accéder aux systèmes d'information participant à l'attaque, d'en collecter les données disponibles et, en tant que de besoin, de mettre en œuvre des mesures visant à neutraliser les effets recherchés par l'attaquant.

Dans le même esprit, le deuxième alinéa de l'article L. 2321-2 du code de la défense, permet aux services désignés par le Premier ministre de détenir des programmes informatiques malveillants, d'en observer le fonctionnement et d'en analyser le comportement. Dans ce cas, il s'agit également de corriger la situation actuelle dans laquelle, en la transposant dans le monde médical, le chercheur n'aurait pas le droit de détenir ou d'étudier un virus pathogène meurtrier afin de fabriquer le vaccin correspondant.

Au-delà de ses aspects organisationnels et techniques, l'article 14 traduit la volonté du Gouvernement de ne pas rester passif face à des attaques informatiques qui portent aujourd'hui atteinte à notre compétitivité et qui demain pourraient mettre gravement en cause notre sécurité ou perturber gravement la vie des Français.

J'en viens à l'article 15 du projet de loi, qui vise à augmenter de manière significative le niveau de sécurité des systèmes d'information des opérateurs d'importance vitale, publics et privés.

Les nouvelles dispositions permettent au Premier ministre d'imposer des règles techniques à ces opérateurs. Il s'agit d'opérateurs « *dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* », selon les termes de l'article L. 1332-1 du code de la défense ; ils sont environ 200. Le Premier ministre pourra également demander des audits ou des contrôles de sécurité à ces opérateurs, qui devront par ailleurs notifier les incidents affectant leurs systèmes d'information. Pour les situations de crise informatique majeure, un article précise que le Premier ministre pourra, lorsque la situation l'impose, les soumettre à des mesures d'exception.

L'expérience opérationnelle de l'ANSSI montre que le niveau de sécurité des systèmes d'information des entreprises et administrations désignées comme opérateurs d'importance vitale est en général insuffisant. Certains systèmes très critiques doivent impérativement être déconnectés de l'Internet pour garantir qu'aucun attaquant ne puisse facilement les pénétrer. Or, l'État n'est pas, à ce jour, en mesure d'imposer une telle règle aux opérateurs concernés. Il est arrivé que l'ANSSI aide une grande entreprise française à reprendre le contrôle de son système d'information et lui conseille la mise en place de règles techniques destinées à renforcer la sécurité de son réseau. Mais il est aussi arrivé qu'elle découvre un peu plus tard que cette même entreprise avait subi une nouvelle attaque car elle n'avait pas appliqué l'ensemble des mesures proposées. Si le projet est adopté, le Premier ministre disposera de la capacité d'imposer des règles de sécurité, organisationnelles ou techniques, susceptibles de renforcer la sécurité des systèmes d'information des opérateurs d'importance vitale. Il pourra par exemple imposer à l'un de ceux-ci d'installer un dispositif de détection d'attaques informatiques.

Comme le Livre blanc le souligne, la capacité à détecter des attaques informatiques relève de la souveraineté nationale. Ce dispositif devra en conséquence s'appuyer sur des équipementiers de confiance labélisés par l'ANSSI, car le concepteur d'un équipement de sécurité est toujours le mieux placé pour le contourner. L'exploitation de ces équipements devra être effectuée sur le territoire national, afin d'éviter toute interception ou

compromission des données, et réalisée par les prestataires qualifiés par l'ANSSI ou par l'ANSSI elle-même.

Le projet de loi instaure aussi une obligation de notification d'incidents affectant le fonctionnement ou la sécurité des systèmes d'information des opérateurs d'importance vitale. À ce jour, la situation est contrastée : les attaques informatiques sont souvent découvertes tardivement. L'expérience acquise par l'ANSSI montre que lorsqu'un opérateur est attaqué à des fins d'espionnage, il est vraisemblable que les opérateurs appartenant au même secteur d'activité subissent, souvent au même moment, les mêmes attaques. Il est donc indispensable que l'État ait connaissance au plus vite de celles-ci afin d'en informer les autres opérateurs du secteur concerné.

Le projet de loi propose aussi d'étendre à l'ensemble des opérateurs d'importance vitale le droit pour le Premier ministre de procéder à des audits ou des contrôles de leurs systèmes d'information. Il est de la responsabilité de l'État de connaître le niveau de sécurité des systèmes d'information des infrastructures critiques de la nation. Aujourd'hui, malheureusement, l'État n'a pas la possibilité d'opérer ou de faire opérer des audits ou des contrôles chez les opérateurs du secteur privé, à l'exception du secteur des communications électroniques. Cette disposition lui permettrait donc de disposer de cette capacité.

Enfin, en cas de crise informatique majeure — par exemple une infection virale destructive touchant nos secteurs d'activité les plus sensibles —, qui exigerait la mise en œuvre de contre-mesures dans des délais courts, la loi donnerait au Premier ministre la possibilité d'imposer des mesures techniques aux opérateurs concernés. L'ANSSI aurait alors la capacité d'imposer les mesures nécessaires pour réagir. L'inscription dans la loi de cette disposition permet également, dans cette circonstance particulière et exceptionnelle, de dégager les opérateurs concernés de leurs responsabilités vis-à-vis de leurs clients.

Des dispositions d'accompagnement complètent ces articles. Elles assurent la confidentialité des informations recueillies dans le cadre des audits. L'effectivité des mesures prescrites est confortée par un dispositif de sanction en cas de manquement après mise en demeure.

En ce qui concerne le contrôle des équipements d'interception, l'article 16 du projet de loi, dont l'actualité révèle la pertinence, vise à mieux maîtriser le risque d'espionnage à grande échelle des réseaux de communications électroniques. Les opérateurs de télécommunication sont tenus de disposer de moyens d'interception afin de répondre, dans le cadre de la loi, aux réquisitions des magistrats pour des interceptions judiciaires, ou du Premier ministre pour les interceptions de sécurité. Les équipements conçus pour réaliser les interceptions présentent un risque pour le respect de la vie privée de nos concitoyens. Ils ne peuvent donc être fabriqués, importés, détenus que sur autorisation délivrée par le Premier ministre, conformément à l'article R. 226-1 et suivants du code pénal. Les interceptions des communications étaient autrefois effectuées par des équipements dédiés. Or, les évolutions technologiques montrent que de plus en plus d'équipements de réseau, sans être des moyens d'interception en eux-mêmes, possèdent des fonctions qui pourraient être aisément utilisées pour intercepter le trafic du réseau.

À cet égard, les fonctions de duplication ou de routage du trafic de certains équipements de réseau, configurables et accessibles à distance, sont susceptibles de permettre des interceptions. Par exemple, certains équipements de cœur de réseau, alors même qu'ils n'ont pas été spécifiquement conçus à des fins d'interception légale, sont susceptibles, selon leurs caractéristiques, de permettre des interceptions du trafic. N'étant pas spécifiquement

conçus pour les interceptions, ces équipements ne sont pas actuellement soumis à l'autorisation prévue par l'article 226-3 du code pénal, qui ne porte que sur les appareils « conçus pour réaliser » les interceptions. Or ces équipements présentent les mêmes risques pour la sécurité des réseaux et des communications que ceux destinés spécifiquement à l'interception. La modification législative qui vous est proposée permettrait donc d'étendre la délivrance d'une autorisation à l'ensemble des équipements susceptibles de permettre ces interceptions, et ainsi d'assurer une plus grande sécurité des réseaux et des communications.

Mme la présidente Patricia Adam. Quels sont les équipements visés par cette nouvelle disposition ?

M. Francis Delon. La loi prévoit que, pour les cœurs de réseau, les équipements destinés à permettre les interceptions de communication pour les besoins légaux que j'évoquais sont soumis à autorisation ; l'ANSSI vérifie qu'ils sont suffisamment robustes pour n'être utilisés qu'à cette fin. Or de plus en plus d'équipements électroniques, qui ne sont pas des cœurs de réseau, notamment des routeurs, peuvent servir à effectuer des interceptions. La loi ne peut fixer la liste des équipements concernés. Elle renverra à des actes réglementaires le soin de le faire. L'intention du Gouvernement n'est pas de contrôler tous les équipements électroniques, ce qui serait impossible, mais de déterminer les plus sensibles. La liste de ces équipements pourra évoluer en fonction de l'évolution des techniques. Nous pourrons vous apporter par écrit des précisions à ce sujet.

Je signale que nous sommes un des rares pays à avoir ce type de dispositions, qui est très efficace, et beaucoup de pays s'y intéressent.

S'agissant du renseignement, le bilan de ces dernières années en matière de connaissance et d'anticipation et les travaux du Livre blanc sur la défense et la sécurité nationale ont montré la pertinence d'élever ce domaine au rang de priorité majeure. C'est ce que fait le projet de LPM dans sa partie programmatique et sa partie normative, sur laquelle je concentrerai mon propos. Les propositions qui y figurent sont la conséquence de cette démarche.

L'effort d'équipement en matière de renseignement vise à conforter nos capacités d'appréciation autonome des situations. Dans le rapport annexé au projet de loi, la priorité est donnée aux composantes spatiales et aériennes, pour l'imagerie et l'interception électromagnétique.

L'effort sur les capacités du renseignement s'accompagne, dans la partie normative du projet de loi, de dispositions visant à clarifier et à renforcer le cadre juridique de l'action des services spécialisés. Les travaux du Livre blanc ont mis en évidence le nécessaire équilibre entre l'accroissement des moyens mis à la disposition des services concernés et leur contrôle démocratique. C'est le sens du renforcement des moyens du contrôle parlementaire sur ce volet de l'activité gouvernementale. Au-delà des dispositions relatives à la Délégation parlementaire au renseignement, sur lesquelles je vais revenir, le Président de la République a souhaité la création d'une inspection du renseignement, commune à l'ensemble des services spécialisés. Les travaux sont engagés pour une mise en place prochaine de cette inspection qui se fera par le biais d'un acte réglementaire.

Le chapitre II de la partie normative du projet de LPM comporte donc diverses dispositions relatives au cadre juridique de l'activité des services de renseignement, qui traitent à la fois de l'accroissement des moyens mis à la disposition de ceux-ci et de leur contrôle démocratique.

Les mesures proposées partent d'un constat : en dépit des efforts importants réalisés, depuis le Livre blanc de 2008, le cadre juridique dans lequel ces services exercent leur activité est encore insuffisant sur plusieurs points pour leur permettre de répondre efficacement aux défis auxquels ils sont confrontés.

Le cadre juridique régissant l'activité des six services spécialisés de renseignement – la DGSE, la DCRI, la DRM, la DPSD, la DNRED et TRACFIN – a été renforcé et précisé par la création en 2007 de la Délégation parlementaire au renseignement et par la précédente loi de programmation militaire du 29 juillet 2009.

Conformément aux recommandations formulées par le Livre blanc de 2008, la gouvernance et la coordination des services de renseignement ont été réorganisées avec la création du Conseil national du renseignement et de la fonction de coordonnateur national du renseignement (CNR).

En 2010, la création de l'académie du renseignement a également permis de doter les services d'une structure de formation commune.

Ces mesures de gouvernance ont été accompagnées d'une réflexion sur les modalités d'action et les moyens mis à la disposition des services. Plusieurs outils ont été créés afin de faciliter l'action de ces derniers et de renforcer la sécurité de leurs agents.

Mais le Livre blanc sur la défense et la sécurité nationale de 2013 va plus loin pour traduire l'importance stratégique de la lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la nation, ainsi que la contribution essentielle qu'apportent à cette lutte les services de renseignement. Il souligne que le renseignement « *joue un rôle central dans la fonction connaissance et anticipation* » et qu'il « *irrigue chacune des autres fonctions stratégiques de notre défense et de notre sécurité nationale* ». Il rappelle aussi les nouveaux défis auxquels doivent s'adapter les services de renseignement et qui les contraignent à s'intéresser à un grand nombre de menaces et à une grande variété d'acteurs aux intérêts parfois convergents – armées régulières, milices, pirates ou mercenaires notamment.

C'est pourquoi, en matière de renseignement, le projet de LPM contient des dispositions sur trois types de sujets : la protection de l'anonymat des agents des services appelés à témoigner, l'accès aux fichiers et la géolocalisation.

La protection de l'anonymat des agents est essentielle, tant pour assurer la sécurité de ceux-ci et de leur famille que pour garantir l'efficacité de leur action. La loi du 14 mars 2011, dite « LOPPSI II », a ouvert aux agents des services de renseignement la possibilité de recourir à une fausse identité ou à une identité d'emprunt. Elle a également inséré dans le code pénal un article protégeant l'identité des personnels, des sources et des collaborateurs des services de renseignement. La procédure actuelle, qui prévoit une protection de l'identité réelle des agents, est cependant, apparue insuffisante. La présence physique de ceux-ci devant une juridiction à la suite d'une convocation et leur participation à des comparutions présentent en effet le risque de dévoiler leur couverture, de mettre en danger leur sécurité et de nuire à l'efficacité de leurs missions. Il a semblé nécessaire de faire évoluer la procédure afin de faciliter la manifestation de la vérité tout en renforçant la protection de l'anonymat des agents. Le projet de loi, en son article 7, prévoit que, dans l'hypothèse où l'autorité hiérarchique de l'agent indique que l'audition comporte des risques pour ce dernier, ses proches ou son service, celle-ci pourra être effectuée dans un lieu assurant la confidentialité et son anonymat.

Par ailleurs, il est prévu d'élargir les conditions d'accès des services de renseignement à certains fichiers administratifs et de police judiciaire. Les menaces auxquelles doivent faire face les services de renseignement dépassent aujourd'hui le seul cadre de la lutte contre le terrorisme. Il s'agit de la prolifération d'armes de destruction massive, de la dissémination d'armes conventionnelles, des menaces des services d'États non coopératifs ou hostiles ou de la criminalité transnationale organisée, notamment. Plus globalement, nos services de renseignement, intérieur et extérieur, s'attachent à préserver les intérêts fondamentaux de la nation. Cette notion est clairement définie dans l'article L. 410-1 du code pénal, qui dispose que « *les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel* ». Par ailleurs, le Conseil d'État, dans un avis du 5 avril 2007, puis le Conseil constitutionnel dans sa décision du 10 novembre 2011 sur le secret de la défense nationale, ont rappelé « *les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la nation* ».

Le projet de LPM comporte, en son article 8, une disposition permettant un accès élargi des services de renseignement aux fichiers administratifs mentionnés à l'article L. 222-1 du code de la sécurité intérieure. Il s'agit des fichiers nationaux des immatriculations, des permis de conduite, des cartes nationales d'identité et des passeports, des dossiers des ressortissants étrangers en France – visa et séjour. Par ailleurs, les motifs de consultation, aujourd'hui limités à la seule prévention des actes de terrorisme, seront étendus à celle des atteintes aux intérêts fondamentaux de la nation. Le texte prévoit qu'un décret en Conseil d'État déterminera les services concernés ainsi que les modalités d'accès. Il est envisagé de faire figurer parmi ces modalités le fait que tous les accès aux fichiers feront l'objet d'une traçabilité et que la Commission nationale de l'informatique et des libertés (CNIL) sera en mesure de les contrôler.

Les articles 11 et 12 permettent aux services de renseignement relevant du ministre de la Défense d'accéder directement à certaines données des fichiers de police judiciaire respectivement dans un objectif de recrutement d'un agent ou de délivrance d'une autorisation aux fins de vérifier le passé pénal du candidat et dans le cadre de missions ou d'interventions présentant des risques pour les agents lorsqu'il s'agit de vérifier la dangerosité des individus approchés. Jusqu'à présent, la consultation de ces fichiers de police judiciaires était possible pour les enquêtes administratives, par l'intermédiaire de policiers ou de gendarmes spécialement habilités à cet effet. L'objectif de cette disposition est notamment de permettre une sécurisation accrue des missions ou des interventions particulièrement dangereuses menées par les services de renseignement du ministère de la Défense. Un décret en Conseil d'État encadrera les conditions d'accès aux fichiers pour s'assurer qu'elles seront adaptées et proportionnées aux besoins des services.

Enfin, l'article 13 du projet de LPM autorise expressément les services de police et de gendarmerie chargés de la prévention du terrorisme à accéder en temps réel à des données de connexion mises à jour, ce qui leur permet de géolocaliser un terminal téléphonique ou informatique et de suivre ainsi, en temps réel, certaines cibles. Cette disposition vise à lever une incertitude sur la base juridique des pratiques de géolocalisation, soulignée par la Commission nationale de contrôle des interceptions de sécurité. Comme le rappelle le rapport de la commission des Lois sur l'évaluation du cadre juridique applicable

aux services de renseignement, « *les services chargés de la lutte contre le terrorisme ont besoin de pouvoir agir le plus en amont possible, au besoin pour écarter d'éventuels soupçons. En outre, il leur faut pouvoir agir en temps réel, dans l'urgence, pour vérifier des renseignements, par exemple sur l'imminence d'un attentat* ». L'accès à ces données répond à un besoin opérationnel de première importance. Ces données sont cruciales pour les services compétents : elles contribuent de façon déterminante aux enquêtes.

Les mesures que je viens d'évoquer élargissent les moyens d'action et de protection des services. Elles appellent un renforcement du contrôle démocratique sur la politique du Gouvernement en matière de renseignement.

C'est pourquoi le projet de LPM, en ses articles 5 et 6, renforce les compétences de la Délégation parlementaire au renseignement (DPR) en modifiant les dispositions de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires ainsi que celles de l'article 154 de la loi de finances pour 2012 du 28 décembre 2011. L'élargissement des compétences de la DPR va dans le sens souhaité par les quatre parlementaires membres du groupe de travail sur le renseignement au sein de la commission du Livre blanc de 2013 et dans celui des préconisations du rapport précité de MM. Jean-Jacques Urvoas et Patrice Verchère.

La DPR avait jusqu'à présent un pouvoir d'information et de suivi. Le projet de LPM innove, en lui confiant un pouvoir de contrôle et d'évaluation de la politique du Gouvernement en matière de renseignement. Le projet de LPM confie à la DPR l'exclusivité, en matière de renseignement, des pouvoirs de contrôle et d'évaluation de l'action du Gouvernement dévolus au Parlement par l'article 24 de la Constitution. Cette disposition respecte le principe de séparation des pouvoirs dont le Conseil constitutionnel a rappelé en 2001 qu'il faisait obstacle à ce que les parlementaires interviennent dans le champ des opérations en cours.

Aujourd'hui, la Délégation peut entendre le Premier ministre, les ministres, le secrétaire général de la défense et la sécurité nationale et les directeurs des services de renseignement. Le projet de LPM permet en outre l'audition du coordonnateur national du renseignement et du directeur de l'académie du renseignement ainsi que celle, après accord des ministres dont ils relèvent, des directeurs d'administration centrale ayant à connaître des activités des services spécialisés de renseignement. Il prévoit également la présentation, par les présidents de la Commission consultative du secret de la défense nationale et de la Commission nationale de contrôle des interceptions de sécurité, du rapport d'activité de leur commission. Le projet de LPM prévoit aussi que la DPR soit informée de la stratégie nationale du renseignement et du Plan national d'orientation du renseignement. Il dispose en outre que seront présentés à la Délégation un rapport annuel de synthèse des crédits du renseignement ainsi que le rapport annuel d'activité de la communauté française du renseignement.

Alors que les dispositions actuelles permettent à la DPR d'adresser des observations au Président de la République et au Premier ministre, le projet de LPM prévoit de permettre à la Délégation d'adresser également à chacun des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget des recommandations et des observations relatives aux services spécialisés de renseignement placés sous leur autorité respective.

Le transfert au profit de la Délégation des compétences de la commission de vérification des fonds spéciaux est un point majeur du dispositif proposé par le

Gouvernement. L'article 6 du projet de loi confie à la DPR les missions de cette commission. Il prévoit que ces missions seront assurées par une « formation spécialisée » de la Délégation, constituée de la moitié des députés et des sénateurs membres de celle-ci. Cette composition restreinte, proche de la composition actuelle de la commission de vérification, répond à l'impératif de stricte confidentialité des informations qui seront examinées par cette formation. Le projet maintient au profit de la formation spécialisée les pouvoirs particulièrement étendus de cette commission, notamment en matière de communication de pièces et de contrôle des documents utiles. Le rapport qu'elle établira sur les conditions d'emploi des crédits sera présenté à l'ensemble des membres de la Délégation.

S'agissant enfin de la création d'un fichier PNR, le domaine de la sûreté aérienne tient une place particulière dans la lutte contre le terrorisme. Tout particulièrement depuis les attentats du 11 septembre 2001, les menaces sur le transport aérien font l'objet d'efforts considérables en matière de sécurité dans le monde entier. Ces efforts portent sur l'ensemble de la sûreté aéroportuaire et s'appliquent aux personnes comme au fret. Comme tout un chacun, terroristes et trafiquants utilisent ce mode de déplacement. Ils savent fractionner leurs itinéraires pour concilier rapidité et discrétion. Or, la particularité du transport aérien est que chaque passager est nominativement enregistré. C'est pourquoi, dès 2004, des dispositions de sécurité ont été élaborées à l'échelle internationale. Elles concernent l'exploitation des données d'embarquement, dites API (*Advance passenger information*), et de réservation, dites PNR. À l'échelon européen, les transporteurs aériens ont obligation de transmettre aux autorités nationales les données API en vertu de la directive 2004/82 du Conseil. En outre, des accords sont en vigueur depuis plusieurs années entre l'Union européenne et les États-Unis, l'Australie et le Canada sur l'échange des données PNR. Nous nous trouvons donc dans la situation paradoxale où trois partenaires utilisent ces données sur des passagers européens pour surveiller les vols entrant et sortant de leur territoire et où nous autorisons leur communication par les transporteurs aériens, alors même que nous ne sommes pas encore en mesure de les exploiter pour notre propre sécurité nationale. Au sein de l'Union européenne, seul le Royaume-Uni exploite les données PNR à grande échelle avec son programme appelé *e-border*. D'autres États, comme les Pays-Bas, la Belgique, la Suède et le Danemark, utilisent ces données, mais sur de plus faibles volumes ou de manière moins automatisée. Comme dans notre pays, ces États sont très attentifs au respect de la vie privée et veillent à l'équilibre entre sécurité collective et libertés individuelles.

En France, la directive européenne de 2004/82 du Conseil a été transposée par la loi anti-terroriste de 2006, qui a élargi le périmètre aux données de réservation PNR, comme la directive l'autorise. En 2010, le Gouvernement a décidé de créer une plateforme d'exploitation des données API et PNR, en s'appuyant sur un projet de directive PNR déposé en février 2011 par la Commission européenne. Ce projet, qui a fait l'objet d'un consensus politique lors du Conseil Justice-Affaires intérieures d'avril 2012, est actuellement soumis à l'examen du Parlement européen. Le Gouvernement français est favorable à son adoption rapide. En attendant, notre pays ne dispose pas à ce jour de dispositif opérationnel qui permettrait d'exploiter ces données. L'article 10 du projet de loi prévoit qu'un tel dispositif soit créé et applicable jusqu'au 31 décembre 2017. Si la directive européenne PNR était adoptée avant 2017, la France la transposerait.

Il est important de préciser l'objectif du dispositif PNR proposé dans le cadre de la LPM ainsi que les garanties prévues pour préserver l'équilibre entre sécurité collective et libertés individuelles. Le dispositif envisagé a pour unique finalité la lutte contre les formes les plus graves de criminalité, à savoir le terrorisme et les crimes graves tels que définis par

l'Union européenne, et de défendre les intérêts supérieurs de la nation, tels que définis dans le code pénal.

La plateforme d'exploitation des données permettra d'effectuer plusieurs opérations. D'abord, le ciblage des passagers sera fondé sur l'analyse du risque à partir de critères objectifs qui permettent de repérer en amont du départ du vol des comportements spécifiques ou atypiques de passagers. Les critères de ciblage, prédéterminés, peuvent être modifiés en fonction de l'évolution des trafics et des modes opératoires des réseaux criminels et terroristes. Les résultats de ce ciblage feront l'objet d'une analyse humaine avant qu'une action de surveillance, de contrôle ou d'interpellation soit décidée.

Le criblage permettra par ailleurs de confronter les données PNR et API aux bases de données utiles à la prévention et à la répression du terrorisme et des formes graves de criminalité, dont les bases de données concernant les personnes et les objets recherchés. Le résultat du criblage est une correspondance potentielle entre les informations croisées, qui pourra être discriminée de façon intelligente afin de réduire le risque d'erreur.

Enfin, l'inclusion des vols intracommunautaires et vers les départements et territoires d'outre-mer est indispensable en raison du fractionnement des déplacements effectués par les terroristes et les trafiquants, à l'image des candidats français au Jihad qui partent rarement directement de Roissy et préfèrent transiter par un pays européen, ou des trafiquants de drogue sud-américains qui transitent souvent par les Antilles.

Les données PNR seront transmises une première fois entre 24 et 48 heures avant le départ du vol. Pendant ce laps de temps, les services pourront exploiter ces données et préparer si nécessaire une éventuelle action de surveillance ou de contrôle. Un second envoi sera effectué à la clôture du vol avec les données API. Il permet de savoir si certains voyageurs ont réservé à la dernière minute, ce qui peut être un indice intéressant pour les services.

Le contenu des données PNR est riche : elles permettent par exemple de savoir à quel moment le passager a réservé son vol et où il a effectué sa réservation. Elles apportent des informations sur l'agence de voyage auprès de laquelle le passager a réservé : certaines de ces agences sont connues des services pour être utilisées par des groupes criminels ou terroristes. Le mode de paiement a également son utilité.

Ainsi, lors de l'enquête sur Mohamed Merah, on a relevé que le dispositif actuel n'avait pas permis d'évaluer la radicalisation de l'intéressé, malgré les informations potentiellement disponibles dans différents fichiers. Pourtant, Mohamed Merah avait suivi une évolution caractéristique en ayant passé plus de six mois au Moyen-Orient en 2010-2011, après avoir emprunté de nombreux vols. Dans ce cas précis, on peut penser que les données PNR auraient permis d'être plus efficace.

Le système envisagé prévoit de nombreuses garanties protectrices des libertés individuelles à chaque étape du traitement des données – collecte, conservation et échanges avec des États partenaires. La mise en place de ce système d'information fera l'objet d'un décret pris en Conseil d'État après avis de la CNIL, qui précisera l'ensemble de ces éléments.

Mme Geneviève Gosselin-Fleury. S'agissant de la disposition permettant au Premier ministre d'imposer des règles aux opérateurs d'importance vitale, est-il prévu, dans le cas d'une modification importante de l'actionnariat de l'un d'eux, que le nouvel actionnaire puisse être agréé par l'ANSSI ou le Premier ministre ? Ainsi, un grand groupe français spécialisé dans l'industrie nucléaire a décidé de mettre en vente sa filiale d'infogérance, qui

gère la conduite informatisée des installations classées. Faut-il prévoir, dans la LPM, que l'acquéreur puisse être soumis à un tel agrément pour s'assurer que cette prise de participation ne débouche sur de l'espionnage ou des cyberattaques ?

M. Francis Delon. La question que vous évoquez est traitée par des dispositions en vigueur sur le contrôle des investissements étrangers dans des secteurs d'activité sensibles. Celles-ci, qui remontent à 2004-2006, sont législatives et réglementaires. Lorsqu'un investisseur étranger non européen veut entrer dans le capital ou prendre le contrôle d'une entreprise de ces secteurs, une procédure permet à l'État de s'y opposer ou de poser des conditions.

M. Christophe Guilloteau. Dans le projet de LPM, seulement 4 articles sur 36 concernent la défense et la plupart, de caractère normatif, intéressent davantage la commission des Lois. Jamais on est allé aussi loin dans la cyberdéfense – ce qui va dans le bon sens –, et on retrouve en matière de renseignement une grande partie du rapport de nos collègues Jean-Jacques Urvoas et Patrice Verchère que vous évoquiez.

Comment voyez-vous le partage des responsabilités en matière de cybersécurité entre l'État et les industriels ?

M. Francis Delon. La partie normative du projet de loi est effectivement ambitieuse, dans le droit fil du Livre blanc.

Si nous allons assez loin dans la sécurité des systèmes d'information (SSI), c'est en s'efforçant d'avoir un dispositif équilibré. Celui-ci ne peut fonctionner qu'avec un partenariat avec l'industrie. Je rappelle qu'il y a beaucoup d'opérateurs d'importance vitale publics et privés et que le texte auquel nous avons abouti résulte d'une concertation avec eux.

Nous avions deux possibilités : maintenir un dispositif incitatif, fondé sur un dialogue avec l'industrie, ou adopter un système plus contraignant. Or beaucoup d'opérateurs nous ont dit que cette seconde option leur rendait service pour mettre en évidence l'importance et le caractère sensible de la sécurité des systèmes d'information, ainsi que pour convaincre leur management et leurs actionnaires – lesquels, j'en suis convaincu, demanderont de plus en plus des comptes aux sociétés sur leur capacité à protéger leurs secrets et leur patrimoine.

L'autre point important dans les relations entre le public et le privé est le partage des tâches dans les opérations de contrôle. L'État ne peut pas tout faire. Nous entendons travailler avec des entreprises françaises, souvent des PME, que nous nous efforçons d'accompagner et avec lesquelles nous avons un rapport de confiance. Cette politique se met en place.

Nous favorisons donc auprès du secteur privé une prise de conscience de l'importance du risque, de la nécessité de se protéger, tout en utilisant au maximum les compétences – nombreuses et de grande qualité – des entreprises françaises.

M. Joaquim Pueyo. Les moyens de la DPR seront-ils suffisants, compte tenu de ses nouvelles missions et de la nécessité de veiller à l'équilibre que vous évoquiez entre la sécurité collective et la protection des libertés ?

M. Francis Delon. Concernant la DPR, il s'agit d'un exercice d'équilibre entre les prérogatives de l'exécutif et celles du Parlement. On essaie de trouver de la façon la plus appropriée le rôle que chacun doit jouer, sachant qu'il faut tenir compte du principe de séparation des pouvoirs.

On donne plus de pouvoirs à la DPR : contrôle à l'égard de la politique du Gouvernement en matière de renseignement ; accès plus large aux faits et aux personnes qu'elle veut entendre. Elle aura une sorte d'exclusivité au sein du Parlement dans ce domaine – résultant notamment de l'absorption de la commission de vérification des fonds spéciaux.

Il revient ensuite au Parlement de déterminer comment et avec quels moyens la délégation travaillera.

S'agissant de l'équilibre entre la sécurité collective et la protection des libertés, le projet de loi est assez précis : on ne donne un accès aux fichiers que pour des finalités particulières et on renvoie à un décret en Conseil d'État le soin d'en préciser les modalités. La CNIL aura par ailleurs son mot à dire.

Les dispositions proposées dans ce domaine ont été pour l'essentiel largement consensuelles et ont donné lieu à assez peu d'arbitrages interministériels.

Mme la présidente Patricia Adam. Je rappelle que la DPR est constituée de huit parlementaires nommés par l'Assemblée nationale et le Sénat, parmi lesquels les présidents des commissions de la Défense et des Lois des deux chambres. Par ailleurs, dans le groupe de travail sur le renseignement de la commission sur le Livre blanc – qui a permis d'élaborer des propositions consensuelles –, quatre parlementaires étaient présents, représentant chacune de celles-ci, ainsi que la majorité et l'opposition.

Il est vrai que la question des moyens se posera. Nous n'avons pas une continuité suffisante du point de vue administratif pour suivre et mettre en place nos travaux.

M. Yves Fromion. Pour avoir été président de la commission de vérification des fonds spéciaux lors de la précédente législature et en être encore membre, j'estime qu'avec quatre parlementaires et deux administrateurs, cette instance a amplement les moyens de remplir ses missions. Mais les parlementaires doivent avoir une certaine disponibilité – en raison des déplacements et des vérifications sur place que la fonction impose –, ce qui me paraît incompatible avec la fonction de président de commission.

Mme la présidente Patricia Adam. La difficulté est qu'aujourd'hui, au sein de la DPR, certains membres font partie de la commission de vérification et d'autres non, ce qui entraîne une inégalité d'accès aux informations et a justifié la fusion entre les deux organismes.

Je pense qu'une formation de la DPR peut effectivement s'occuper de la vérification des fonds spéciaux, ce qui implique en effet de la part des parlementaires concernés une certaine disponibilité. Selon moi, il revient à la Délégation de nommer les quatre collègues chargés de cette mission en tenant compte de cette contrainte.

Quant à la composition de la DPR, j'estime important que certains présidents de commission en fassent partie de droit.

M. Olivier Audibert Troin. Sur les sept chapitres du projet de LPM, le premier est programmatique et les six autres portent davantage sur le cadre juridique à proprement parler. La cyberdéfense est affichée comme étant une, voire la priorité nationale. L'article 14 fait du Premier ministre le pivot dans ce domaine. Si, selon l'article L. 2321-1 du code de la défense, il reviendra au Premier ministre de définir et coordonner l'action gouvernementale en matière de sécurité – ce qui est conforme notamment à l'article 20 de la Constitution –, au titre de l'article L. 2321-2, les services de l'État pourront, dans les conditions fixées par le Premier ministre, engager tout type d'action pour répondre à une attaque des systèmes

d’information portant atteinte au potentiel de guerre, à la sécurité ou à la capacité de survie de la nation. N’y a-t-il pas un glissement des prérogatives du Président de la République – qui est le chef des armées au titre de l’article 15 de la Constitution – vers le Premier ministre ?

M. Francis Delon. L’organisation actuelle en matière de cyberdéfense s’appuie déjà sur le Premier ministre. Outre qu’il en a constitutionnellement la responsabilité, en pratique, le SGDSN assure cette mission au travers de l’ANSSI. Le projet de loi s’inscrit donc dans la continuité du dispositif existant, permettant au Premier ministre d’avoir une vue d’ensemble sur l’ensemble des services de l’État.

Dans l’hypothèse d’une attaque majeure, il n’y aurait pas de contradiction avec les pouvoirs dévolus par la Constitution au Président de la République. On ne vise pas dans le projet une attaque militaire. Il s’agit d’une attaque informatique d’une importance telle qu’elle nécessite une action immédiate et coordonnée, qu’il incomberait au Premier ministre d’assumer au travers de l’ANSSI.

M. Jean-Jacques Candelier. Le rôle du SGDSN est très important. Mais les moyens prévus par le projet de loi seront-ils suffisants pour répondre à ses attentes dans le contexte actuel ?

Pensez-vous que ce projet renforcera la sécurité des Français ?

Enfin, disposerons-nous de moyens efficaces vis-à-vis des 150 à 200 jeunes Français partis auprès des djihadistes en Syrie, dont certains reviendront ?

M. Francis Delon. S’agissant des moyens, je ne peux me prononcer que sur la sécurité des systèmes d’information. Un effort très important est fait dans ce domaine par le Gouvernement : les effectifs de l’ANSSI passeront de 350 à 500 personnes d’ici la fin de 2014 et les crédits augmenteront également substantiellement. Il serait donc malvenu que je me plaigne !

Je pense que le projet de loi amél

iorera la sécurité des Français, que ce soit au travers de la sécurité des systèmes d’information, du renseignement ou des données PNR.

Quant aux filières de terroristes se dirigeant vers la Syrie, elles sont un sujet de préoccupation constant de nos services de renseignement. Nous veillons à ce qu’elles ne se développent pas et en tirons toutes les conséquences en termes de sécurité intérieure.

M. Francis Hillmeyer. Comment l’ANSSI, qui est une agence de sécurité civile, peut-elle agir dans le domaine militaire ?

M. Jacques Lamblin. Vous avez indiqué qu’un espionnage massif était pratiqué par des institutions nationales, faisant allusion à l’armée chinoise. Pouvez-vous nous dire quels sont les autres pays ou institutions s’adonnant à ce type d’activité ?

Par ailleurs, le projet de loi permettra la collecte d’un maximum de renseignements. Or, on voit qu’aux États-Unis, la masse des informations recueillies est telle qu’ils n’ont pas la capacité de les analyser. Quel équilibre doit-on trouver entre la collecte et la capacité d’analyse des renseignements ?

M. Francis Delon. L’ANSSI a une compétence globale sur l’ensemble du champ d’action de l’État, y compris le domaine de la défense. Cela étant, chaque ministère est fortement incité à avoir des capacités pour ses besoins propres. C’est le cas de celui de la défense, où existe un dispositif de cyberdéfense spécifique.

Les relations entre l'ANSSI et les ministères sont parfaitement organisées et fonctionnent bien, y compris avec le ministère de la Défense. Du fait de la croissance de ses effectifs, une partie des services de l'ANSSI vient d'ailleurs d'emménager dans de nouveaux locaux et y accueille le CALID, qui est le service de ce ministère chargé de la cyberdéfense. Cela facilite la communication entre les deux.

Monsieur Lamblin, je n'ai pas dit que l'armée chinoise nous attaquait : j'ai seulement indiqué que le rapport *Mandiant* parlait des attaques chinoises.

Les attaquants viennent de plusieurs pays – que je ne peux citer ici en raison de la publication du compte rendu de cette audition.

Il faut en effet bien prendre en compte à la fois les capacités de recueil et d'analyse des renseignements. Mais la France n'est pas dans la situation des États-Unis : elle dispose de bonnes capacités de collecte des informations et est, à ma connaissance, en mesure de traiter celles-ci.

M. Philippe Folliot. Les articles 17 à 20 du projet de LPM me paraissent importants, même si on en parle peu. Alors que nous connaissons une judiciarisation de notre société, ils tendent à protéger l'action militaire, qui est par définition spécifique. Vont-ils assez loin dans ce domaine, au regard notamment des suites judiciaires données aux faits survenus dans la vallée d'Uzbeen ?

Par ailleurs, certaines opérations sont menées dans un cadre juridique particulier : c'est le cas pour les actions de lutte contre l'orpaillage clandestin en Guyane, qui s'apparentent à des opérations extérieures (OPEX) alors qu'elles sont effectuées sur le territoire national en temps de paix. N'y a-t-il pas un vide juridique en la matière vis-à-vis de la protection de nos forces et de nos hommes ?

M. Yves Foulon. Quels sont les moyens concrets prévus pour s'assurer de la protection de nos concitoyens vis-à-vis des interceptions de communications ?

M. Francis Delon. Monsieur Folliot, je n'ai pas évoqué les articles 17 à 20 du projet de loi, qui portent sur le traitement pénal des affaires militaires, car il m'a semblé plus légitime qu'ils vous soient présentés par le ministère de la Défense.

Cela étant, il se trouve que j'ai présidé le groupe de travail sur les questions de judiciarisation. L'objet de ces dispositions – qui concernent tous les engagements extérieurs, y compris les opérations spéciales, et ont été débattues de façon approfondie avec les ministères de la Défense et de la Justice – est précisément d'éviter qu'il y ait un nouvel Uzbeen judiciaire. Le traitement pénal de cette affaire a créé un choc dans les armées et suscité la crainte que l'action militaire, si spécifique, soit traitée de la même manière qu'une activité professionnelle ordinaire. L'aspect exceptionnel des actions de combat nous a semblé insuffisamment pris en compte.

Je pense que nous avons trouvé le bon équilibre. Il ne s'agit pas d'introduire une immunité absolue : naturellement, si un événement tout à fait anormal se produisait dans une OPEX, il pourra donner lieu à un traitement pénal. Mais celui-ci ne sera pas systématique.

Il est vrai que l'opération Harpie en Guyane que vous évoquez n'est pas couverte par ces dispositions. Faut-il qu'elle le soit ? Nous n'avons pas étudié la question, qu'il faudra poser aux ministères de la Défense et de la Justice.

Monsieur Foulon, nous nous efforçons de faire en sorte que nos concitoyens ne puissent pas être espionnés de façon illégale en utilisant des matériels installés sur les réseaux.

C’est la raison pour laquelle nous contrôlons les cœurs de réseau. Mais comme nous constatons que les matériels permettent de plus en plus d’opérer des interceptions, nous étendons le contrôle que nous exerçons sur eux.

Je ne dis pas que cela donne une garantie absolue à nos concitoyens de ne pouvoir être espionnés. Mais les dispositions proposées prennent en compte l’évolution des techniques et améliorent la protection globale de nos concitoyens.

La séance est levée à onze heures cinquante-cinq.

*

* *

Membres présents ou excusés

Présents. - Mme Patricia Adam, M. François André, M. Olivier Audibert Troin, M. Sylvain Berrios, M. Daniel Boisserie, M. Jean-Jacques Candelier, Mme Nathalie Chabanne, M. Guy Chambefort, M. Luc Chatel, M. Jean-Louis Costes, Mme Catherine Coutelle, M. Bernard Deflesselles, M. Lucien Degauchy, M. Philippe Folliot, M. Jean-Pierre Fougerat, M. Yves Foulon, M. Yves Fromion, Mme Geneviève Gosselin-Fleury, Mme Edith Gueugneau, M. Christophe Guilloteau, M. Francis Hillmeyer, M. Patrick Labaune, M. Jacques Lamblin, M. Charles de La Verpillière, M. Gilbert Le Bris, M. Maurice Leroy, M. Philippe Meunier, M. Jacques Moignard, M. Philippe Nauche, Mme Sylvie Pichot, Mme Émilienne Poumirol, M. Joaquim Pueyo, M. Eduardo Rihan Cypel, M. Gwendal Rouillard, M. Jean-Michel Villaumé, M. Philippe Vitel

Excusés. - M. Ibrahim Aboubacar, M. Claude Bartolone, M. Philippe Briand, M. Alain Chrétien, M. Guy Delcourt, M. Éric Jalton, M. Jean-Yves Le Déaut, M. Frédéric Lefebvre, M. Bruno Le Roux, M. Alain Marleix, M. Damien Meslot, Mme Marie Récalde, M. François de Rugy, Mme Paola Zanetti