ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique

– Table ronde sur les libertés et les activités de renseignement avec M. Jean-Marie Delarue, président de la commission nationale de contrôle des interceptions de sécurité (CNCIS), et M. Jean-Jacques Urvoas, président de la commission des lois de l'Assemblée nationale, membre de la CNCIS 2

– Audition de M. Jean-Marc Manach, journaliste, spécialiste des questions de surveillance et de vie privée sur Internet, auteur du blog *Bug Brother* 17

Jeudi
13 novembre 2014
Séance de 8 heures 30

Compte rendu n° 07

SESSION ORDINAIRE DE **2014-2015**

Présidence de Mme Christiane Féral-Schuhl,
coprésidente
Et de
M. Christian Paul,
coprésident

ASSEMBLÉE NATIONALE

COMMISSION DE RÉFLEXION ET DE PROPOSITIONS SUR LE DROIT ET LES LIBERTÉS À L'ÂGE DU NUMÉRIQUE

Jeudi 13 novembre 2014

La séance est ouverte à huit heures quarante.

(Présidence de Mme Christiane Féral-Schuhl, co-présidente et de M. Christian Paul, co-président)

Table ronde, sur les libertés et les activités de renseignement, avec M. Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), et M. Jean-Jacques Urvoas, président de la commission des lois de l'Assemblée nationale et de la délégation parlementaire au renseignement, membre de la CNCIS

M. le coprésident Christian Paul. Notre table ronde de ce matin évoquera les activités de renseignement, leur déploiement sur les réseaux numériques, le cadre juridique et les dispositifs de contrôle applicables à ces activités. Nous auditionnerons M. Jean-Jacques Urvoas, moins, d'ailleurs, en tant que président de la commission des lois de l'Assemblée nationale qu'en tant que président de la délégation parlementaire au renseignement (DPR) et membre de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), ainsi que M. Jean-Marie Delarue, président, depuis quelques mois, de la CNCIS. Le troisième intervenant prévu, M. le préfet Alain Zabulon, coordonnateur du renseignement auprès du Président de la République, n'a finalement pu être là ce matin ; j'espère que nous pourrons l'auditionner avant la fin de l'année. Cette table ronde est publique : elle est retransmise sur le site de l'Assemblée et fera l'objet d'un compte rendu.

Les réseaux numériques ayant pris une place importante dans la vie de tout un chacun, la question des activités de renseignement sur ces réseaux est devenue importante, notamment avec l'apparition de questions liées à la criminalité et au terrorisme. Certains excès et débordements de ces activités ont par ailleurs inquiété l'opinion. La commercialisation par la France, en dehors de tout contrôle, d'outils de surveillance des réseaux, notamment à la Libye dans les années 2000, a ainsi suscité un profond mécontentement citoyen. De même, l'affaire Snowden, à la suite des révélations par un analyste de la CIA de la manière dont le renseignement américain procède en dehors des États-Unis, a soulevé bien des questions, notamment en France.

Nous souhaitons avoir, ce matin, un état des lieux sur les méthodes du renseignement français et les principales technologies qu'utilise celui-ci, qu'il s'agisse de l'interception du contenu des communications ou de celle des métadonnées de connexion. De même, l'encadrement juridique de ces activités est-il suffisant ? Les droits fondamentaux sont-ils bien protégés ? Enfin, les capacités de surveillance et d'intrusion des nouvelles technologies étant considérables, les moyens du contrôle démocratique sont-ils à la hauteur ?

M. Jean-Jacques Urvoas, président de la commission des lois de l'Assemblée nationale et de la délégation parlementaire au renseignement, membre de la Commission nationale de contrôle des interceptions de sécurité. Mon propos sera, avant tout, le résultat d'observations personnelles, dans un domaine dont je ne prétends pas être

spécialiste, étant simplement un parlementaire investi d'une responsabilité sur des sujets encore très largement ignorés par le Parlement lui-même. Le travail que mène cette Commission est utile car notre pays a toujours été relativement indifférent à ces questions. Il n'existe pas en France, à la différence de la plupart des démocraties occidentales, de culture du renseignement. Nous éprouvons, et c'est étonnant, une forme de défiance envers ces services, alors que ceux-ci sont avant tout l'outil d'une politique publique au service de l'intérêt général.

Je suis partisan d'une confrontation apaisée des opinions sur le sujet. Les questions sont certes sensibles, et les conditions de l'exercice de ces activités à l'ère numérique posent des questions nouvelles qui n'existaient pas auparavant ; la quête de l'information est en effet de plus en plus dépendante des outils technologiques, de la captation d'images aux interceptions électromagnétiques et numériques. Le terrain est propice aux psychoses, aux fantasmes, aux illusions, et il faut tâcher de les combattre par le droit, c'est-à-dire par la préservation des libertés individuelles.

C'est précisément l'une des fonctions de la délégation parlementaire au renseignement, dont je suis le président cette année. Il s'agit d'une structure bicamérale où siègent quatre sénateurs et quatre députés, avec une présidence tournante. C'est le président de la commission des affaires étrangères, de la défense et des forces armées du Sénat, M. Jean-Pierre Raffarin, qui me succédera l'an prochain, et j'ai moi-même succédé au président de la commission des lois du Sénat, M. Jean-Pierre Sueur. Notre mission est précisée par la loi : nous avons vocation à organiser le contrôle parlementaire de l'action du Gouvernement en matière de renseignement et d'évaluer la politique publique en ce domaine.

C'est également la mission de la CNCIS, même si le champ de celle-ci est limité aux interceptions de sécurité dans le domaine administratif. Il s'agit d'une structure où je siège depuis le début de la législature, et pour toute sa durée, le mandat étant par ailleurs non reconductible.

Mes observations se résument en deux idées fortes. Je constate, tout d'abord, que l'espionnage massif et multiforme n'est ni dans la culture ni dans les moyens de nos services. La France, dans ce domaine, se veut une puissance souveraine, quand la Grande-Bretagne se vit plutôt comme un allié, très aligné, des États-Unis. Nous n'appartenons pas aux *Five Eyes*, ce cercle de mutualisation des moyens du renseignement réunissant depuis très longtemps les États-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande, et qui a été le socle de la solidité du bloc occidental au cours de la Guerre froide. Cette volonté d'autonomie et de souveraineté de la part de notre pays nous conduit à penser qu'il est absurde de chercher à comparer nos outils et ceux de ces puissances. Les budgets sont sans commune mesure : le budget de la seule *National Security Agency* (NSA), par exemple, l'une des seize agences de renseignement américaines, serait cinquante fois supérieur à celui de notre direction générale de la sécurité extérieure (DGSE).

Nous avons également une philosophie singulière. Là où les États-Unis et la Grande-Bretagne ont développé une confiance aveugle dans le renseignement technique, la France a maintenu une préférence pour le renseignement humain. Le principal outil de la Grande-Bretagne, le *Government Communications Headquarters* (GCHQ), compte six mille spécialistes du travail d'écoute. La France a toujours considéré que sa situation géographique, y compris en outre-mer, et son histoire, avec des zones d'influence privilégiées, impliquait le recours au renseignement humain comme principal canal.

Enfin, le cadre juridique dans lequel nos services évoluent est incroyablement restrictif, par rapport aux États-Unis par exemple. Vous savez comme moi que 95 % de l'action de la NSA est légale ; la justice fédérale américaine a d'ailleurs rappelé, en décembre dernier, que la collecte de métadonnées correspondait à la mission de l'agence. Les révélations de M. Snowden n'ont donc été des révélations que pour ceux qui ne connaissaient pas ce sujet.

Deuxième point : en vue de renforcer la protection des libertés individuelles, la délégation parlementaire considère qu'il faut une loi sur le renseignement. Notre pays aujourd'hui n'en a pas. Le cadre, notamment s'agissant du contrôle, est insuffisant. Il convient d'encadrer l'action des services, donc de développer le contrôle, et ce en multipliant les organes.

Le contrôle interne, c'est-à-dire le contrôle hiérarchique exercé par l'autorité ministérielle sur ses services, n'existait pas avant que le Président de la République pallie cette carence en créant, le 25 juillet 2014, l'Inspection du renseignement. Il ne s'agit pas d'un nouveau corps comme l'Inspection générale de la police nationale, l'Inspection générale de la gendarmerie nationale ou l'Inspection générale des finances, mais d'une instance de contrôle qui réunit des fonctionnaires de ces inspections habilités à connaître de telles questions. Ce contrôle existe désormais et doit à présent démontrer son efficacité.

Le deuxième contrôle est le contrôle parlementaire, par le biais de la délégation parlementaire au renseignement (DPR). Notre structure a été créée en 2007, sous la précédente législature ; elle n'était alors dotée que d'un pouvoir de suivi de l'activité des services. Depuis la loi de programmation militaire du 18 décembre 2013, la DPR contrôle désormais, comme je l'ai indiqué, l'action du Gouvernement en matière de renseignement. Nous rendrons notre premier rapport dans un mois, à la mi-décembre. Les données consultables depuis 2007 sur les sites de l'Assemblée nationale et du Sénat sont plus des notes que des rapports. J'espère que notre rapport convaincra l'opinion de l'investissement des parlementaires dans le contrôle de cette politique publique.

Il reste selon nous un contrôle à créer, que nous appelons contrôle de légalité et de proportionnalité, devant examiner si les moyens mis en œuvre par les services sont proportionnés à la menace qu'ils sont censés combattre. De notre point de vue, c'est la vocation d'une structure comme la CNCIS, dont le champ est actuellement trop restrictif. Il faut faire disparaître la CNCIS en tant que telle pour la recréer, avec un périmètre élargi, sous la forme de ce que le Conseil d'État nomme une autorité de contrôle des services de renseignement, appellation qui me semble peu explicite et que je suggère donc de remplacer par « autorité de contrôle des techniques de renseignement ».

Il convient par ailleurs d'ouvrir des voies de recours pour les citoyens. Ces voies de recours ne peuvent avoir pour fondement que la loi. Si la France ne se dote pas d'une loi, elle sera un jour condamnée. J'espère donc que l'année 2015 permettra de délibérer d'un tel texte, dans des conditions qui ne soient pas celles d'une confrontation de fantasmagories, mais permettent l'expression d'une volonté commune de protéger les libertés individuelles.

Enfin, les sociétés privées, dans le domaine du renseignement, suscitent des inquiétudes, car leur activité est autrement plus débridée que celle des services, et il existe des dangers, notamment concernant la communication des données personnelles. C'est un sujet sur lequel le législateur serait également bien inspiré de se pencher.

M. le coprésident Christian Paul. La question du contrôle, vous l'avez dit, est essentielle ; celle de la nature même des activités de renseignement et des techniques auxquelles elles recourent ne l'est pas moins. Vous avez, dans le débat public, opposé des activités massives, que vous avez appelées « pêche au chalut », et des activités plus ciblées, que vous avez appelées « pêche au harpon ». Qu'est-ce qui relève, dans l'activité de nos services aujourd'hui, de l'une et de l'autre ?

M. Jean-Jacques Urvoas. S'agissant d'activités classifiées, mon propos ne peut avoir la liberté que nous avons au sein de la DPR dans nos relations avec les directeurs des services. Notre activité se fonde sur les informations qui parviennent à notre connaissance et, lorsque nous avons une interrogation, nous essayons de remonter à la source pour vérifier l'information. Toutes les informations qu'il m'est arrivé de lire sur les activités de renseignement ne sont pas corroborées par notre observation.

Pendant longtemps, la suspicion a été de mise entre le Parlement et les services de renseignement. Pour une grande partie des parlementaires, les services de renseignement étaient les fils naturels des affaires Ben Barka et *Rainbow Warrior*, et par nature liberticides. De leur côté, ces services avaient tendance à considérer les parlementaires comme des bavards impénitents, dépourvus de tout souci de l'intérêt général et seulement préoccupés par leur notoriété. La création de la délégation parlementaire au renseignement a permis à ces deux mondes de se connaître, et la confiance a pu s'instaurer.

Dans le cadre des activités de la DPR, aucune porte n'a été fermée, aucun refus ne nous a été opposé ; nous nous sommes rendus là où nous le souhaitions et nous avons rencontré qui nous voulions. Le cadre de notre activité n'est toutefois pas sans limites. Ces limites ont notamment été fixées par le Conseil constitutionnel, en 2001. Le gouvernement de Lionel Jospin avait souhaité créer la Commission de vérification des fonds spéciaux, où devaient siéger à la fois des parlementaires et des magistrats de la Cour des comptes. Les sénateurs ont saisi le Conseil en invoquant le fait que ce n'était pas le rôle du Parlement de s'intéresser aux fonds spéciaux. Le Conseil leur a donné raison et conclu que le Parlement ne devait pas avoir accès aux « opérations en cours », sans préciser ce dont il s'agit. Il peut donc arriver, hypothétiquement, qu'un service oppose à l'une de nos demandes le motif d'une opération en cours. S'il y a des opérations en cours, je n'y ai pas accès, et je ne le souhaite pas puisque le Conseil constitutionnel me l'interdit ; pour le reste, jamais un directeur de service n'a entravé nos recherches.

M. le coprésident Christian Paul. Je m'autorise un droit de suite sur ce point. Ma question portait davantage sur la notion de « proportionnalité » dans votre propos. Si nous débattons prochainement d'une loi sur le renseignement, comment garantir à nos concitoyens que ces activités resteront proportionnées aux diverses menaces, quand, dans d'autres pays – nous l'avons vu pour les États-Unis –, le caractère massif de la surveillance, sur les métadonnées et sans doute aussi les contenus, est visiblement dépourvu de tout caractère de proportionnalité ?

M. Jean-Jacques Urvoas. La définition de la proportionnalité ne peut découler que des missions confiées aux services. Or, aujourd'hui, la loi ne précise pas ces missions. Le décret créant la DGSE, en 1982, est l'un des premiers qui aient été publiés au *Journal officiel* dans ce domaine. Tant que les missions ne sont pas définies, je ne peux apprécier la proportionnalité des actions conduites. C'est pourquoi il faut une loi, cohérente, définissant les missions confiées aux services, les outils dont ceux-ci doivent disposer, les instances de

contrôle, et la manière dont les agents de ces services sont protégés dans l'exercice de leurs fonctions.

La seule loi existant aujourd'hui dans le domaine du renseignement est la loi de 1991 sur les interceptions de sécurité. Cette loi a été très bien conçue, sous la responsabilité de Daniel Vaillant, car elle a permis au contrôle de s'adapter aux évolutions technologiques, alors que l'usage des téléphones portables et des moyens numériques dont nous parlons était encore inexistant à l'époque. Aujourd'hui, la CNCIS contrôle les interceptions de sécurité sur ces outils.

M. Edwy Plenel. Nous sommes face à une révolution industrielle qui non seulement bouleverse nos réalités économiques et culturelles mais modifie aussi profondément les questions relatives aux libertés et aux possibilités d'attenter à celles-ci. Vous pouvez chanter la fable des différences entre les moyens de notre pays et ceux d'autres puissances ; il n'en demeure pas moins que les moyens techniques sont sans frontières.

Vous avez commencé par dire qu'il existait en France une grande indifférence au renseignement, un mépris envers celui-ci. Je suis de ceux qui pensent, au contraire de vous, que cette indifférence est liée à la faiblesse de notre culture démocratique. Les puissances qui ont une culture du renseignement sont en même temps celles où sont conduits des *hearings* publics, brutaux, des responsables du renseignement, et où les parlementaires vont jusqu'au bout de leur pouvoir, au service des citoyens et non de secrets illégitimes.

Quand il s'est agi d'entrer dans le concret, vous avez aussitôt brandi les secrets classifiés, dont vous seriez le gardien, dans une attitude opposant les « sachants » aux ignorants. Vous défendez ainsi ce qui est, selon moi, la perdition de la démocratie, à savoir l'entre-soi de ceux qui savent mieux que le peuple et ne souhaitent pas que le peuple sache.

La question n'est pas tant celle du mépris du renseignement que celle de l'usage abusif de ces services par le pouvoir exécutif et de l'abandon du contrôle parlementaire. Il n'y a pas eu de commission d'enquête parlementaire sur l'affaire *Greenpeace*, alors que les exécutants auraient été contents de montrer qu'ils n'avaient fait que leur travail, sur ordre du pouvoir. Il n'y a pas eu de commission d'enquête, ni même de saisine de la Commission nationale de l'informatique et des libertés (CNIL), sur la cellule antiterroriste de l'Élysée qui a détourné les moyens de l'État au service d'une privatisation de la Présidence de la République. Pas de commission d'enquête non plus sur l'action de nos services de renseignement dans l'aventure libyenne, action qui, de l'avis même de ceux qui y ont participé, est au cœur du dérapage de ces opérations. Pas de commission d'enquête non plus sur le scandale des « fadettes », échappant au contrôle de la CNCIS, alors que leur usage abusif violait les droits de la presse. Nos interpellations sont au service des gardiens du secret : pour que les secrets soient bien gardés, en démocratie, il faut une culture démocratique.

M. Delarue a été nommé par le pouvoir exécutif, vous cumulez, monsieur Urvoas, diverses fonctions – membre de la CNCIS, président de la commission des lois de l'Assemblée, président de la délégation parlementaire au renseignement –, et M. Zabulon coordonne le renseignement au cœur du pouvoir exécutif : ce tableau montre une imbrication des pouvoirs, non une séparation, alors que cette dernière est pourtant nécessaire à un exercice effectif du contrôle. Une loi sur le renseignement est très légitime à condition que l'on favorise en même temps l'extension des droits et des libertés à l'âge du numérique, droit de

savoir, droit d'accès à l'information… Le meilleur contrôle est celui de la société, plus que celui de ses représentants.

Votre discours serait plus convaincant si vous acceptiez qu'il existe en France, dans votre domaine, la même chose que dans les autres grandes démocraties. Nous en avons débattu ici même, et c'est pourquoi les auditions de cette commission sont publiques : pourquoi, dans le domaine du renseignement ou de la défense, n'avez-vous pas renforcé la publicité des auditions de responsables ? Qui, mieux que les gens des services, peut nous informer de ce que fait le Gouvernement ? Qui, mieux que les officiers de la gendarmerie présents au moment des faits, peut nous informer de ce qui s'est passé à Sivens, pour connaître les ordres qu'a donnés, *via* le préfet, le Gouvernement, et qu'il cherche à cacher ? Comme le disait Bailly, « la publicité est la sauvegarde du peuple ».

Pourquoi vous opposez-vous, en tant que président de la commission des lois, au projet de loi sur la protection réelle du secret des sources des journalistes ? Ce projet a été débattu il y a un an ; les professionnels de l'information ont été entendus. Selon ce que des parlementaires nous ont indiqué, alors même que vous défendez l'idée d'une loi sur le renseignement, vous faites partie de ceux qui font obstacle au respect de cette promesse de votre majorité.

De même, allez-vous agir pour remettre en cause l'extension illégitime, sous la précédente majorité, du secret défense à des lieux comprenant certains lieux privés tels que des sites d'entreprises liées aux industries de défense ? Ces lieux sont interdits non seulement à la curiosité des journalistes et des citoyens, mais aussi à celle des juges, et cette interdiction n'est pas remise en cause par l'actuelle majorité. Nous avons toujours été, en France, du côté du secret. Je rappelle que c'est une campagne de presse qui a permis à la France de se doter, après quelques condamnations de la Cour européenne des droits de l'homme, d'une loi sur les interceptions de sécurité, et à la CNCIS d'exister.

Enfin, que savez-vous, puisque vous êtes un « sachant », des liens entre nos services et les sociétés privées ? Nous pensons que certaines sociétés sont des sous-traitants de nos services, permettant à ceux-ci de conduire des opérations à l'abri d'un statut privé ? Vous avez vous-même souligné que ces sociétés allaient plus loin que ce qu'il est possible à nos services de faire. Pouvez-vous nous assurer, publiquement, que les sociétés *Amesys*, qui avait des contrats en Libye, et *Qosmos*, en Syrie, sociétés spécialistes du *deep packet inspection*, une technologie qui permet de pénétrer en profondeur dans les systèmes numériques, n'ont pas de liens avec notre appareil de sécurité, ni avec notre politique extérieure ? Si de telles sociétés ont pu violer les libertés sous des dictatures, elles peuvent mettre leurs instruments au service de certains abus chez nous aussi.

M. Philippe Aigrain. Si vous avez évoqué la préoccupation des libertés individuelles, monsieur Urvoas, notre commission a également le souci de certaines libertés collectives. Nous avons ainsi considéré que les articles 10 à 15 de la loi relative à la lutte contre le terrorisme pouvaient s'appliquer à toute forme d'action politique collective radicalisée, donc au-delà des seules actions terroristes.

Par ailleurs, si la France n'appartient pas aux *Five Eyes*, nous savons que la vision de la NSA et du GCHQ est celle de cercles concentriques, et que, dans le deuxième cercle, la France est considérée comme un partenaire privilégié, même si les relations sont très asymétriques. Les commentateurs, les personnes qui exploitent les documents d'Edward Snowden ou de Duncan Campbell, soulignent que, si la France n'occupe pas une position centrale dans ce système, elle n'en est pas absente.

Vous avez affirmé que les révélations d'Edward Snowden n'auraient appris des choses qu'à ceux qui n'ont pas assez travaillé sur ces questions. Sur le contenu même des informations, sur l'existence d'une surveillance généralisée, c'est vrai. Ces révélations apportent néanmoins la preuve que ce qu'affirmaient les groupes de défense des libertés fondamentales aux États-Unis, à savoir que le *Foreign Intelligence Surveillance Act* (FISA), bien qu'assorti en apparence de contrôles juridiques sérieux, ouvre la porte à la surveillance généralisée par le biais de toute une série de programmes de surveillance, dont la liste se monterait actuellement à quatre cents, avaient raison. Les insultes aux défenseurs des libertés, traités de paranoïaques, le traitement infligé à de hauts responsables de la NSA qui critiquaient là une dérive, témoignaient en réalité d'un aveuglement des contrôleurs.

La question, ensuite, de l'action des sociétés privées en matière de renseignement ne concerne pas seulement les atteintes très importantes à la déontologie des données de la vie privée par les grands intermédiaires de l'internet. Il s'agit certes d'un sujet de préoccupation majeur de cette commission, que nous espérons voir traité dans une loi, mais nous constatons aussi que les prestataires ou, dans le cas de partenariats public-privé, les partenaires privés des services et de l'administration sont source de risques.

Dans un contexte de faits non classifiés mais soumis à une obligation de confidentialité, j'ai eu l'occasion d'auditionner des responsables de services, quand la France, à l'occasion de l'élaboration du Livre blanc sur la défense, cherchait à redéfinir sa politique à l'égard de la sécurité dans le cyberespace. Il semble qu'un très grand nombre de risques proviennent de pressions imaginées par les services eux-mêmes, souhaitant prouver leur utilité. Le risque de dérive des services tient souvent aux formes d'interaction entre le pouvoir politique et ces services. Les services de la sécurité intérieure occupent à cet égard une place particulière, par rapport à ceux de la sécurité extérieure.

J'en viens à quelques questions. Vous avez indiqué que la DPR n'intervenait que sur ce dont elle était informée, en essayant de remonter à la source. Pouvez-vous préciser les modalités de cette remontée à la source ? S'il se fait jour une surveillance en voie de généralisation – c'est ainsi que j'appelle une surveillance qui aimerait être généralisée, au même niveau que les pays anglo-saxons, mais qui se heurte à des limites budgétaires –, si une telle dérive, vers une surveillance généralisée des communications sur internet, s'amorce, comment les instances de contrôle en auraient-elles connaissance ou, à tout le moins, pourraient-elles le soupçonner ?

En cas d'attribution de nouveaux pouvoirs à des services de police ou de sécurité, il est à notre sens raisonnable de considérer l'hypothèse qu'ils en abusent. L'histoire des services de sécurité semble montrer que ce n'est pas seulement une éventualité, mais plutôt une constante, dans tous les pays. Or, lorsque, dans le cadre de cette commission, nous avons auditionné des membres du cabinet de M. Cazeneuve, un tel point de vue a suscité des difficultés de dialogue, alors même que c'est un point de vue nécessaire pour pouvoir être réactif.

Enfin, il est fréquent que des parlementaires qui ont participé aux débats aboutissant à la création d'autorités de contrôle, y soient nommés. Par exemple, M. Riester et M. Thiollière, rapporteurs respectifs de la loi créant la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI) dans les deux chambres, ont été nommés membres de cette autorité ; depuis lors, je ne sache pas qu'ils aient été particulièrement actifs dans les débats sensibles. Nous avons considéré qu'il y avait là une forme d'atteinte à la séparation des pouvoirs, ou de conflit d'intérêts, mais cela ne semble pas être votre opinion. Qu'en est-il ?

M. Jean-Jacques Urvoas. Dans la future loi relative au renseignement, l'autorité administrative indépendante (AAI) qui sera chargée du contrôle de proportionnalité ne devra pas compter de parlementaires en son sein. En effet, on ne peut évaluer que les situations que l'on a connues. Nous devons poursuivre notre réflexion sur la question du contrôle, car il ne faut pas conférer aux structures des responsabilités qu'elles ne sont pas capables d'assumer. Qui contrôlerait la proportionnalité d'une extension de la surveillance ? Le Parlement ne pourrait pas remplir ce rôle, car ses membres ne possèdent ni les compétences techniques indispensables ni le temps nécessaire. Les personnes désignées pour siéger dans cette AAI devront y officier à temps plein pour que le contrôle s'effectue efficacement.

Il n'y a pas de mépris pour le renseignement en France, mais un nuage de suspicion s'est formé car on parle toujours des échecs des services et jamais de leurs succès. Les services de renseignement sont indispensables à la démocratie et ils ont bien tort de ne pas faire connaître leurs réussites. Quelle fut leur action en Somalie pour récupérer notre otage, M. Denis Allex ? Je l'ignore, mais je suis convaincu qu'ils ont entrepris tout ce qui était possible, animés du patriotisme qui les habite. La DPR a demandé à M. Jean-Marc Ayrault, alors Premier ministre, d'engager des poursuites contre les journaux ayant publié le nom de celui qui dirigeait le commando ayant tenté de libérer M. Denis Allex ; il s'agissait en effet d'une infraction à la loi qui méritait une suite judiciaire.

Lors de la précédente législature, la commission des lois a examiné un texte relatif au secret des sources. Les amendements, nombreux, furent très discutés, et en particulier celui portant sur la définition des intérêts fondamentaux de la nation – terminologie que la Cour européenne des droits de l'homme (CEDH) n'accepte plus, contraignant ainsi le législateur français à la préciser. La commission des lois a émis des propositions pour modifier la loi, mais le Gouvernement n'a pas encore inscrit ce texte à l'ordre du jour malgré ma demande écrite.

M. Edwy Plenel. À quelle date avez-vous adressé cette requête au Gouvernement ?

M. Jean-Jacques Urvoas. Il y a quinze jours.

M. Edwy Plenel. À la suite, donc, de l'épisode de *Valeurs actuelles* qui a ému les rédactions et les sociétés de journalistes du fait de la violation du secret des sources.

M. Jean-Jacques Urvoas. Il n'y a aucun lien entre les deux événements.

Je ne suis pas un « sachant », monsieur Plenel, mais j'exerce une responsabilité qui ne durera que le temps de mon mandat, alors que l'on doit construire une architecture garantissant la pérennité du contrôle.

Il est légitime de rendre plus crédible le contrôle parlementaire. Or l'habilitation au secret défense empêche de répondre à certaines questions, sous peine d'enfreindre la loi ; comment, dès lors, vérifier l'efficacité du contrôle ? La fonction de contrôle parlementaire des services de renseignement est récente, si bien qu'il est normal que nous tâtonnions. Nous avons souhaité bénéficier de l'expérience des Américains et des Britanniques en la matière ; la délégation parlementaire au renseignement s'est ainsi entretenue avec le président de l'*Intelligence and Security committee* de la Chambre des Communes – cette structure disposant d'un budget et de moyens humains incomparables aux nôtres – et avec la présidente de la commission du contrôle du renseignement au Sénat des États-Unis, Mme Dianne Feinstein. Tous deux nous ont mis en garde contre les auditions publiques, qui ne servent qu'à diffuser les informations que les services veulent porter à la connaissance de tous. Parce que l'intention ne suffit pas et que nous avons besoin de preuves, il faudra associer l'ensemble des parlementaires aux travaux de la délégation. Pour notre premier rapport, nous avons choisi quatre thèmes : le renseignement économique et financier ; les politiques de ressources humaines dans les services de renseignement ; le cadre juridique des services ; l'état du monde après les révélations de M. Edward Snowden. Le rapport et les suites que le Gouvernement y donnera constitueront le test de la crédibilité du contrôle parlementaire.

Le Conseil constitutionnel a partiellement censuré le texte voté en 2011 sur l'extension du secret défense à des lieux. Le Gouvernement ne m'a pas fait savoir qu'il souhaitait reprendre ce texte, et la commission des lois ne travaille pas non plus sur ce sujet en ce moment.

À l'occasion de la révision constitutionnelle de 2008, ma famille politique s'était opposée à ce que l'on prenne prétexte de l'existence d'une enquête judiciaire pour s'opposer à la création d'une commission d'enquête. Je continue de défendre la position qui était la nôtre et souhaite voir disparaître cette exception française. Depuis le début de cette législature, notre majorité ne refuse pas les demandes formulées par l'opposition, contrairement à la précédente majorité ; une commission parlementaire vise à repérer les lacunes de la législation, alors que les magistrats cherchent à établir les responsabilités dans la commission de faits : leurs fonctions sont donc de nature différente.

Depuis que je suis président de la délégation parlementaire au renseignement, je n'ai jamais rencontré la structure *Qosmos-Amesys* et on ne me l'a jamais présentée comme un prestataire des organismes que nous rencontrons.

M. Edwy Plenel. Accepteriez-vous également une commission d'enquête sur les événements de Sivens ?

M. Jean-Jacques Urvoas. La commission des lois a décidé de créer une mission d'information sur les unités de forces mobiles il y a trois semaines. Les faits auxquels vous faites allusion entreront dans son champ d'étude, qui englobera les doctrines d'emploi, les moyens mis à la disposition des escadrons de gendarmerie, des compagnies républicaines de sécurité (CRS) et des compagnies départementales d'intervention (CDI), l'implantation des casernes et les rémunérations.

Mme la coprésidente Christiane Féral-Schuhl. Combien d'avis émettez-vous chaque année ? Parmi eux, combien sont négatifs ?

M. Jean-Jacques Urvoas. Nous publions un rapport, mais nous n'émettons pas d'avis. La délégation parlementaire se réunit chaque jeudi, le travail de cette première année, de nature principalement méthodologique, ayant visé à élaborer des pratiques vertueuses pour l'avenir. Nous avons ainsi défini de manière extensive la communauté du renseignement en y incluant la direction du renseignement de la préfecture de police de Paris – qui possède les mêmes compétences que la direction générale de la sécurité intérieure (DGSI) dans le territoire francilien –, le service central du renseignement territorial (SCRT) et la sous-direction à l'anticipation opérationnelle (SDAO) de la direction générale de la gendarmerie nationale (DGGN). Le rapport sera rendu à la fin du mois de décembre comme il sied à tout rapport annuel.

M. Philippe Aigrain. Avez-vous à connaître de l'activité d'opérateurs privés, par exemple de télécommunications, offrant des prestations aux services de renseignement ?

M. Jean-Jacques Urvoas. Si nous en ressentions le besoin, nous pourrions le faire.

M. Philippe Aigrain. Je vous y invite.

M. le coprésident Christian Paul. Monsieur Delarue, la loi de 1991 a-t-elle bien vieilli ? S'avère-t-elle capable d'épouser l'évolution profonde des technologies d'interception ? Ce cadre juridique préserve-t-il les libertés ? La Commission nationale de contrôle des interceptions de sécurité dispose-t-elle de moyens suffisants pour exercer sa mission ?

M. Jean-Marie Delarue, **président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).** Je vous remercie de me donner l'occasion de réfléchir avec vous sur ces questions difficiles qui concernent les droits de chacun – respect de la vie privée, de la correspondance, du domicile, des données personnelles –, droits protégés par les normes juridiques internes, même si des lacunes existent, et internationales, ainsi que les nécessités constitutionnelles de la préservation de l'ordre public. L'équilibre s'avère délicat, et il convient, pour le maintenir, que la loi définisse les objectifs, les garanties des citoyens et les recours dont ils disposent.

La loi du 10 juillet 1991 relative aux interceptions de sécurité a créé un dispositif auquel mes prédécesseurs à la tête de la CNCIS ont insufflé un dynamisme protecteur. Ce texte, tardif, fut élaboré contre la volonté des pouvoirs publics et sous la pression de la société et des critiques de la CEDH. Le premier rapport sur la question fut commandé dans l'enthousiasme de 1981, mais il n'a débouché que dix ans plus tard, ce qui n'est pas à notre honneur. La loi de 1991 comporte des dispositions intéressantes car elle protège, dans son article 1er, le principe du secret des correspondances et, donc, des communications électroniques ; tout ce qui entrave ce principe attente aux libertés. Elle circonscrit les motifs pour lesquels on peut porter atteinte à cette protection ; au nombre de cinq, ces justifications précisent les notions trop vagues dont ne se contente plus la CEDH, comme celle des intérêts fondamentaux, pourtant définie par le code pénal. Le texte plafonne le nombre d'interceptions, le Premier ministre décidant du contingent ; celui-ci n'est pas annuel, et le Premier ministre peut l'augmenter après avoir requis notre avis, souvent réticent. La dernière hausse du contingent date de janvier dernier, et 2 190 personnes sont aujourd'hui susceptibles de faire l'objet d'interceptions de sécurité. La loi sépare l'autorité demandant l'interception – les ministres – de celle les décidant – le Premier ministre. La durée de conservation des enregistrements des écoutes ne peut excéder dix jours, cette question ayant fait l'objet de

débats nourris au moment du vote de la loi. Je me suis opposé à ce que le récent projet de loi de prévention du terrorisme allonge cette durée et je me réjouis que cette disposition ait finalement été abandonnée. La loi de 1991 permet la transcription des seuls enregistrements ayant reçu une autorisation, les interceptions touchant à la vie privée ne pouvant être conservés. Enfin, le texte a créé l'AAI que je préside aujourd'hui ; celle-ci est chargée de donner un avis au Premier ministre sur toutes les demandes d'interceptions, de contrôler la réalisation de celles-ci et d'accueillir toutes les réclamations des citoyens. Elle est représentée à la commission dite « R. 226 » qui contrôle les matériels utilisés par les services.

En vingt-trois ans d'existence, la CNCIS a montré son indépendance et inscrit son action au-delà de la lettre de la loi. Ainsi, alors que celle-ci prévoyait que l'avis de la Commission soit donné postérieurement à la décision du Premier ministre, la pratique a consacré son caractère préalable. Cet avis se fonde sur une analyse des demandes des services transmises par le groupement interministériel de contrôle (GIC), service du Premier ministre chargé de l'exécution des interceptions ; la CNCIS contrôle l'adéquation entre les faits et les conditions posées par la loi, elle vérifie qu'ils reposent sur une présomption aussi solide que possible et elle examine l'implication directe et personnelle de l'individu faisant l'objet de la requête. Elle exige que les présomptions soient solidement établies, qu'elles se trouvent en rapport précis avec l'un des motifs retenus par la loi, et que la personne soit directement impliquée. Veuillez m'excuser d'insister sur ce point, mais il se situe au cœur de notre action.

Si le Premier ministre jouit théoriquement d'une liberté de décision absolue, il a toujours suivi, à quelques exceptions près, les avis de la Commission.

La CNCIS ne se contente pas de transmettre un avis positif ou négatif, elle les assortit de recommandations portant, par exemple, sur un raccourcissement de la durée d'écoute – la loi la fixe à quatre mois, mais la Commission se prononce pour un temps plus court dans quelques cas précis. De même, la CNCIS demande souvent que son autorisation soit soumise à la production des enregistrements par le GIC, afin de vérifier que ceux-ci sont bien conformes à l'objectif fixé et que les transcriptions ne sont pas indûment étendues.

La Commission a également pris l'habitude de vérifier sur place les conditions dans lesquelles les interceptions s'effectuent ; nous visitons ainsi une quinzaine de fois par an les centres dans lesquels on procède aux écoutes. Elle rencontre également les opérateurs par lesquels passe la saisine de données. Il existe donc bien un contrôle postérieur à l'autorisation, qui vise à vérifier la façon dont celle-ci est mise en œuvre.

Une jurisprudence relative aux autorisations s'est progressivement constituée ; elle cherche avant tout à défendre les libertés individuelles des citoyens et à contrôler la portée des atteintes à ces libertés, en prenant en compte l'état du droit en France, les exigences de la CEDH et les limites que l'on ne peut franchir sous aucun prétexte. Pour ma part, mon unique mission consiste à appliquer l'intégralité de la loi dans le respect des droits de chacun.

Le dispositif actuel s'avère néanmoins insatisfaisant, puisque l'équilibre des années 1990 est rompu. Notre société se révèle plus sensible au besoin de sécurité – le droit à la sécurité fut reconnu par la loi en 1995, donc postérieurement à celle relative aux interceptions. Les composantes de la menace ont évolué avec l'émergence d'une dimension terroriste qui n'existait pas en 1991. La criminalité internationale est devenue plus difficile à appréhender, et les moyens de communication se sont considérablement développés puisque ni *Google ni Facebook* n'existaient en 1991. Les services se sont adaptés à ce contexte et peuvent déployer de nouvelles méthodes intrusives, non encadrées par le législateur et n'offrant pas de garanties

aux citoyens. Cette situation concerne autant le champ administratif que celui des interceptions judiciaires ; ces dernières, qui représentent un volume dix fois supérieur aux interceptions administratives, ont été élargies à d'autres domaines, et la CEDH se montre vigilante face à l'utilisation de certaines techniques non encadrées par la loi.

Au-delà de l'affaiblissement des garanties, point la tentation d'élaborer une loi pour chaque technique. Ainsi, la loi de prévention du terrorisme du 23 janvier 2006 a permis la saisine de métadonnées, dont l'autorisation a été confiée à une personnalité qualifiée, placée auprès du ministre de l'intérieur, et sur l'indépendance de laquelle il y a lieu de s'interroger. La loi de programmation militaire (LPM) a élargi ce dispositif, et cette personnalité qualifiée aura également à connaître, à partir du 1er janvier prochain, de la saisine de métadonnées pour les cinq items posés par la loi de 1991. La CNCIS n'effectue dans ces domaines qu'un contrôle *a posteriori*, la personnalité délivrant les autorisations. Je regrette l'existence de ce système.

On a justifié les différences de régime juridique entre les interceptions de sécurité et les métadonnées par le caractère moins intrusif des secondes. C'était sans doute vrai il y a quelques années, mais la situation a changé. La saisine répétitive et portant sur des domaines étendus de métadonnées apporte beaucoup d'informations, d'autant plus précieuses que ceux qui pensent être l'objet d'interceptions de sécurité sont discrets dans leurs propos. Tout contrôle doit offrir des garanties d'indépendance, et les procédures de saisine des métadonnées en sont actuellement dépourvues. Il convient donc de faire évoluer la loi en la matière, même si les motivations pour conduire cette modification s'avèrent des plus diverses.

Une future loi ne devra pas avoir vocation à régir les services de renseignement. L'article 34 de la Constitution n'oblige pas le Gouvernement à soumettre à la loi l'organisation de ses services, fussent-ils de police. En revanche, il appartient à la loi de trancher sur l'ensemble des libertés individuelles ; elle devra donc réaffirmer la protection de ces libertés au regard des technologies actuelles et des atteintes qui peuvent leur être portées. La CEDH, notamment dans son arrêt du 31 août 2005 *Vetter contre France*, est d'ailleurs allée dans le même sens en fournissant des indications très précises sur ce que la loi doit disposer en la matière.

La loi devra clairement définir les conditions et les motifs auxquels une atteinte aux libertés individuelles peut être conduite. S'agissant des justifications, je ne me contenterai pas d'un simple renvoi aux intérêts fondamentaux de la nation, la CEDH exigeant une précision bien supérieure.

La loi devra réaffirmer le principe de subsidiarité, qui veut que les atteintes aux libertés individuelles ne soient autorisées que s'il s'avère impossible d'employer un autre moyen.

La contrepartie naturelle de la loi réside dans l'arrêt de toute pratique des services se situant hors de son champ. Il y a lieu de renforcer la sanction pénale des infractions résultant d'actions illégales.

La loi devra régler la délicate question des opérations des services dans des pays étrangers. Le champ de la loi française est territorial, mais il convient de réfléchir aux moyens de limiter l'usage d'interceptions à l'étranger réalisées par les autorités françaises.

La loi devra poser le principe de l'unité du contrôle des différentes atteintes aux libertés individuelles. Cela ne signifie pas que le contrôle parlementaire et celui interne aux services doivent cesser – il y a même lieu de développer ce dernier –, mais que celui exercé par une personne indépendante soit regroupé. Celle-ci devra être indépendante du pouvoir et exercer son contrôle sur l'ensemble des services – il faudra donc privilégier une approche organique plutôt que matérielle. Ce contrôle devra porter sur l'ensemble des atteintes aux libertés et être conduit *a priori* et *a posteriori*, la loi devant poser le principe d'un avis préalable et garantir l'exercice d'un contrôle sur pièces et sur place de la réalisation des saisines de données. Le contrôle ne devra comporter aucun caractère décisionnel, les autorités politiques devant prendre leurs responsabilités. Enfin, il devra respecter les besoins des services, notamment s'agissant de la rapidité et de la discrétion de leur action.

La loi devra distinguer entre la demande d'un service, l'avis fourni par une autorité de contrôle, la décision du politique et le contrôle de l'exécution des atteintes aux libertés individuelles par un organe indépendant des services de renseignement et de police. Cette architecture existe en matière d'interceptions de sécurité, et il convient de l'étendre aux éventuelles atteintes nouvelles que la loi pourra définir.

M. le coprésident Christian Paul. Le Conseil d'État a évoqué dans un récent rapport la possibilité d'instaurer un signalement des activités illégales depuis l'intérieur des services et à l'attention de l'autorité de contrôle. Quelle est votre opinion sur cette question ?

Quelles digues solides peut-on ériger contre les tentations de surveillance généralisée par stockage massif de données ?

M. Philippe Aigrain. Monsieur Delarue, je tiens à vous remercier pour la clarté et le contenu de votre riche intervention, qui aurait été utile d'entendre au moment du débat sur l'article 20 de la LPM.

La Cour de justice de l'Union européenne (CJUE) a invalidé la directive 2006/24 du 15 mars 2006 sur la conservation des données, car certaines de ses dispositions lui paraissaient attenter de manière disproportionnée aux droits fondamentaux. Le droit interne intègre-t-il bien les motivations de cette décision ?

Je souscris totalement à votre propos sur l'érosion de la pertinence de la distinction entre les effets de la capture des métadonnées et de celle des contenus. La pseudo-garantie de transmission des métadonnées aux opérateurs présente en fait un très grand risque. Votre contrôle devra donc englober ces intermédiaires privés, ce qui soulèvera des questions de mise en œuvre importantes.

M. Edwy Plenel. Monsieur Delarue, votre intervention rejoint notre prisme qui est celui des libertés.

La loi sur les interceptions date de 1991, époque où seules les conversations téléphoniques étaient concernées. On intercepte maintenant des agendas, des lieux et des courriers électroniques avec une grande facilité. Comment vivez-vous votre impuissance à contrôler l'ensemble de ces interceptions ?

L'affaire des « fadettes » a suscité un émoi dans votre Commission et une intervention du Premier ministre de l'époque. Une structure a été installée dans les locaux de l'ancienne direction centrale du renseignement intérieur (DCRI) pour étudier les factures

détaillées de certaines personnes : est-ce la personne qualifiée au ministère de l'intérieur, ou un agent de la DCRI, qui validait les demandes en circuit court ?

La multiplication des AAI a dessaisi le Parlement de sa fonction de contrôle, ce qui pose un problème d'indépendance dans notre démocratie présidentielle. Votre Commission a connu un baptême du feu difficile à l'occasion d'un scandale d'interception de sécurité qui concernait directement la présidence de la République. La CNCIS n'a pas conquis sa totale indépendance à cette occasion, et il a fallu engager une procédure judiciaire pour régler cette affaire. Comment garantir structurellement l'indépendance de la CNCIS, au-delà de l'éthique personnelle de ses membres ?

M. Winston Maxwell. Une disposition de la loi de 1991 exclut des mécanismes de contrôle la surveillance généralisée des ondes hertziennes ; devrait-on la modifier à l'occasion d'une future réforme du texte ?

M. Jean-Marie Delarue. Les personnes dans les services peuvent saisir la CNCIS et n'ont pas besoin d'une autorisation législative pour ce faire. J'accorde bien plus de mérite aux autorités de contrôle interne qu'aux hérauts et héros se sacrifiant pour la cause d'autrui : je crois à l'intérêt des lanceurs d'alerte, mais j'ai encore plus de foi dans un contrôle interne méthodique et incontestable. Le groupement interministériel de contrôle (GIC) dispose depuis quelques années d'une cellule de contrôle interne avec laquelle la CNCIS travaille en étroite collaboration. Les services doivent organiser en leur sein une structure juridique et une autre dédiée au contrôle, et tous n'en sont pas encore dotés.

La surveillance n'est pas généralisée, mais ciblée ; la loi de 1991 précise que les demandes sont adressées sur des personnes déterminées. Il n'existe pas de requête portant sur une collectivité, même si les mesures individuelles ne portent pas sur un numéro de téléphone, mais sur l'ensemble des téléphones des 2 190 personnes ciblées. En revanche, la loi devra se pencher sur les pratiques déployées à l'étranger pour les faire entrer dans le droit touchant les interceptions pratiquées dans le territoire national.

L'arrêt de la CJUE, *Digital Rights contre Irlande*, est susceptible de double interprétation. Si l'on retient l'interprétation maximaliste, on peut en effet lire cette décision comme une limite sérieuse à la conservation des données. La Cour de justice ne s'est pas prononcée sur une durée précise et n'a pas condamné celle d'une année posée par le code des postes et des communications électroniques aux opérateurs. Cette durée ne semble pas exorbitante *a priori* et doit s'adapter au caractère intrusif du contenu des données. Les durées de conservation ne doivent pas être trop longues en effet, mais elles doivent permettre d'utiliser les données recueillies. Le principe est que plus l'intrusion est forte, plus la durée doit être courte. On doit adapter celle-ci aux besoins identifiés – et non hypothétiques pendant une longue période – des services.

La réputation de plus faible intrusion des métadonnées dans la vie des individus ne me convainc pas plus que vous. Est-ce plus intrusif de savoir si quelqu'un se rend à la mosquée ou aux *Galeries Lafayette* le vendredi ? On ne peut ni répondre à cette question à la place d'autrui ni élaborer une règle sur ce fondement. Il convient de considérer toute saisie d'information sur la vie personnelle de manière uniforme.

Monsieur Plenel, je ne me sens pas impuissant dans ma tâche de contrôle. Dans les avis que nous adressons au Premier ministre, nous utilisons une large palette de modulations et demandons des éléments précis si nous nourrissons un doute sur l'une des conditions que

doit remplir la requête d'interception ; sur ce fondement, nous pouvons adresser des recommandations au Premier ministre pour cesser immédiatement l'interception. Si un service demande une interception, reçoit l'autorisation de l'effectuer, mais ne réalise aucune transcription, alors nous lui envoyons une notification d'interruption de l'interception puisque celle-ci ne s'avérait pas nécessaire. Sans faire preuve de naïveté et en restant très vigilant, peu nous échappe en matière d'interception de sécurité.

Je n'hésiterai pas à utiliser l'article 40 du code de procédure pénale si j'ai connaissance de pratiques qui n'ont pas lieu d'être – que celles-ci émanent des services, des autorités politiques ou de la CNCIS. S'agissant de l'affaire dite des fadettes, le Parlement et la juridiction compétente ont entendu mon prédécesseur, M. Hervé Pelletier, qui a fourni les explications qu'il pensait devoir donner. Je n'ai rien à dire de plus à ce sujet, si ce n'est que je ferai tout pour éviter qu'une autre affaire de cette nature ne se reproduise.

Je crois à la vertu des AAI, mais l'indépendance morale ne suffit en effet pas. La loi future devra renforcer les garanties objectives qui permettent de définir l'indépendance de l'institution, car celle-ci ne se présume pas. La loi doit expliciter le fait que la CNCIS ne reçoit d'instruction d'aucune autorité et ne se soumet qu'au contrôle de la Cour des comptes. La norme légale doit également poser des incompatibilités entre certaines fonctions et celle de membre de la Commission.

La loi de 1991 – codifiée sur ce point à l'article L. 241-3 du code de la sécurité intérieure – a prévu d'excepter certains coups de téléphone du contrôle de la CNCIS relevant des intérêts diplomatiques supérieurs de la France. Portant uniquement sur les communications hertziennes, cette disposition a perdu toute portée et n'aura donc pas à figurer dans la loi future.

M. Philippe Aigrain. Vous avez évoqué le contrôle des pratiques se déroulant à l'étranger. Qu'entendez-vous par là ? Faites-vous allusion aux communications captées à l'étranger, qui peuvent être effectuées en France par le biais d'applications comme *Skype* ou *Google Talk* et qui peuvent être transmises aux services français, ou aux activités des services de renseignement à l'étranger ?

M. Jean-Marie Delarue. Parmi les communications téléphoniques, il y a celles qui se déroulent entre deux personnes se trouvant dans le territoire national, celles entre une personne en France et une autre à l'étranger, celles entre une personne à l'étranger et une autre en France et celles entre deux personnes à l'étranger. La CNCIS a à connaître des trois premières catégories, mais, comme j'imagine mal que les services se désintéressent de la quatrième, la loi doit encadrer leurs pratiques.

M. Philippe Aigrain. La surveillance n'est ni complètement ciblée ni totalement généralisée. Il s'agit d'un régime hybride qui détermine les cibles de manière automatisée. Le récent projet de loi renforçant la prévention et la répression du terrorisme reprend d'ailleurs cette approche.

M. Jean-Marie Delarue. Toutes les interceptions de sécurité en France ont pour objet une personne déterminée ; tout autre dispositif sortirait du cadre de la loi.

M. Edwy Plenel. Une interception sur les téléphones d'une seule personne peut conduire à collecter des données sur beaucoup de monde.

M. Jean-Marie Delarue. En effet, mais une demande d'interception s'accompagne de la liste des numéros de téléphone – qui, dans les faits, n'excède jamais dix numéros par personne – dont les communications seront interceptées, et les services nous avisent de tout changement dans la liste. La Commission a donc connaissance de toute extension du dispositif d'interception.

M. Godefroy Beauvallet. L'intérêt pour une personne pourrait être éveillé par la surveillance de contenus publics ou semi-publics en provenant des réseaux sociaux comme *Facebook et Twitter*. Ne doit-on pas examiner le lien entre ce qui relève de l'interception et ce qui a trait à la veille sur ces données ?

M. Jean-Marie Delarue. Les technologies ont certes évolué, mais les techniques des services également. L'interception de sécurité arrive ainsi au bout de la chaîne de surveillance, après la saisie d'informations accessibles à tous et après celle des métadonnées. C'est pourquoi la loi doit promouvoir l'unicité du contrôle ; il convient d'éviter la situation dans laquelle une personnalité qualifiée autoriserait une opération que la CNCIS refuserait en aval du processus, car elle permettrait aux services d'accumuler des données de manière illégitime. Or, pour le dire clairement, il s'agit là de la tentation des dernières années.

Puis la Commission procède à l'audition de M. Jean-Marc Manach, journaliste, spécialiste des questions de surveillance et de vie privée sur Internet, auteur du blog « Bug Brother »

M. le coprésident Christian Paul. Monsieur Manach, soyez le bienvenu. Compte tenu de vos travaux et de votre engagement, votre audition fait le lien avec la précédente, consacrée aux activités de renseignement et d'interception de communications électroniques, et plus généralement aux remparts à ériger contre ce qu'il est convenu d'appeler la société de surveillance. Comment percevez-vous la situation, et quelles sont vos éventuelles recommandations en ce domaine ? Nous souhaitons d'abord vous entendre sur le cas de la France, même si l'on sait, notamment depuis l'affaire Snowden, que ces questions dépassent largement ses frontières.

Je rappelle que cette séance est retransmise sur le site de l'Assemblée nationale.

M. Jean-Marc Manach, journaliste, spécialiste des questions de surveillance et de vie privée sur Internet, auteur du blog « Bug Brother ». Merci de votre invitation. Journaliste sur Internet, j'ai commencé à me pencher sur les questions dont nous parlons au moment des révélations de Duncan Campbell sur le système *Echelon*. En 2001, aucun guide n'existait pour expliquer au grand public comment utiliser les outils de chiffrement : c'est en traduisant des modes d'emploi que je me suis familiarisé avec les systèmes de surveillance des télécommunications, et appris comment on pouvait s'en protéger. J'ai ainsi été conduit, notamment, à travailler sur l'affaire *Amesys*, entreprise française qui a conçu un système de surveillance de masse au profit du régime de Mouammar Kadhafi.

Lors de ma précédente audition dans cette enceinte, au lendemain des premières révélations de l'affaire Snowden sur l'interception des métadonnées par la National Security Agency (NSA), j'avais parlé d'« hystérie médiatique » car, si ces révélations n'étaient pas nouvelles, c'est la première fois qu'elles acquéraient une dimension médiatique mondiale ; depuis, le volume des documents révélés par Edward Snowden m'a conduit à revenir sur cette expression. Naguère, lorsque j'évoquais la « société de surveillance », on m'accusait souvent de paranoïa ; mais depuis l'affaire Snowden, tout le monde est devenu paranoïaque, et c'est bien le problème. Beaucoup de gens ont entendu dire dans les médias que la NSA espionne

tout et, parce qu'ils ignorent le fonctionnement des systèmes de surveillance, en ont conclu que la Direction générale de la sécurité extérieure (DGSE) en faisait de même sur notre sol : c'est ce que laissait entendre, en juillet dernier, un article à la une du journal *Le Monde*. Il reposait sur l'un de mes propres articles, publié suite à une conférence du directeur technique de la DGSE, qui expliquait que la France était dans le « top 5 » des nations en matière d'interception des télécommunications. Après vérification, j'en suis arrivé à la conclusion que, si la DGSE est en effet capable d'espionnage à grande échelle, elle ne surveille pas l'intégralité des télécommunications en France : cela se verrait.

Ces vérifications, j'ai été amené à les faire à trois reprises, suite à des unes du *Monde* qui se sont révélées fausses, s'agissant par exemple de la prétendue surveillance, par la NSA, de 70 millions de communications téléphoniques en France – en réalité, il s'agit de métadonnées captées par la DGSE à l'étranger, et partagées avec son homologue américaine. On a aussi prétendu que la société *Orange* était un partenaire privilégié du *Government communications headquarters* (GCHQ), auquel elle fournirait des données relatives à ses abonnées français. Je n'ai pas de preuves que c'est faux, mais beaucoup d'indices me laissent plutôt penser que le GCHQ s'intéresse bien davantage aux clients d'Orange établis au Mali ou au Nigeria qu'à ceux qui le sont sur notre sol. Pourquoi, de plus, *Le Monde* n'évoquait-il que les abonnés français ? L'explication tient sans doute à la paranoïa que les révélations d'Edward Snowden ont suscitée : certains se sont réveillés avec, passez-moi l'expression, une « gueule de bois » qui leur inspire une défiance générale. Cette attitude est dangereuse en démocratie.

Même si j'ai un certain nombre d'idées sur le sujet, j'ignore les pratiques des services de renseignement en France ; en tout état de cause, si la surveillance devait être massive, elle serait plutôt le fait de la Direction générale de la sécurité intérieure (DGSI) que de la DGSE. Toutefois, aucun indice ne me conduit à penser que les services de renseignement français violent la loi, et je n'ai pas de raison de douter des propos de M. Delarue. Selon ses dires, toute interception, en France, s'opère sur une personne déterminée ; mais *quid*, alors, des « *IMSI-catcher » (International Mobile Subscriber Identity*), qui, semblables à des cellules téléphoniques, permettent d'intercepter les numéros de tous les utilisateurs situés dans leur zone ? J'ignore si les services utilisent de tels appareils – comme le font, à en croire la presse américaine, des forces de police aux États-Unis –, profitant ainsi de la loi de 1991 – qui exclut la surveillance du spectre hertzien du contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) – pour identifier des manifestants à Sivens, à Notre-Dame-des-Landes ou près de certaines mosquées. C'est en tout cas une possibilité que leur offre notre droit.

La culture du renseignement fait cruellement défaut. J'ai moi-même eu à me former à la sécurité informatique, auprès de hackers, afin de protéger mes sources. Les professionnels soumis au devoir de confidentialité découvriront, sur le site de la Commission nationale de l'informatique et des libertés (CNIL), comment leurs communications peuvent laisser des traces sur Internet, mais pas comment les protéger. Le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) contient également un guide du voyageur, où il est recommandé, lors des déplacements à l'étranger, d'utiliser un ordinateur vierge, de se connecter *via* un réseau privé virtuel – *virtual private network*, VPN – aux données restées en France, puis, une fois revenu, de confier l'ordinateur au responsable de la sécurité informatique de l'entreprise ou de l'administration afin de vérifier qu'aucun logiciel espion n'a été installé. Créé en 2008 seulement, le portail « securite-informatique.gouv.fr » n'a pas été mis à jour depuis décembre 2013, alors qu'il s'est passé beaucoup de choses en la matière depuis cette date. Il n'existe à ce jour aucun manuel grand public pour expliquer, notamment

aux personnes soumises au secret professionnel, comment protéger les données. Le problème n'est pas législatif mais politique, car on ne pourra jamais dissuader les services des grands pays de mener des opérations d'espionnage ; c'est donc aux usagers eux-mêmes de se protéger à travers le chiffrement, dont nous répétons depuis des années qu'il devrait être une fonctionnalité par défaut des logiciels. L'affaire Snowden est de nature à favoriser l'écoute de notre message par les pouvoirs publics et économiques ; jamais autant d'informaticiens n'ont œuvré à « durcir l'Internet », selon le mot de Bruce Schneier. Il faut faire en sorte que l'accumulation des couches de cryptage rende toute surveillance inutile : bien que la NSA ou la DGSE, entre autres, aient engagé de vastes campagnes pour déjouer le chiffrement, nos idées ont le vent en poupe, ce qui n'était pas le cas avant l'affaire Snowden.

M. Edwy Plenel. Culture du renseignement et culture démocratique vont de pair : c'est le droit de savoir qui est en jeu, moyennant bien entendu la protection légitime de certains secrets. L'entreprise *Qosmos* a mené, en Syrie, des opérations similaires à celles d'*Amesys* en Libye, grâce à la technologie d'inspection des paquets en profondeur, dite « DPI », et ce jusqu'en 2012 au moins. J'ai demandé à M. Urvoas, parlementaire chargé du contrôle en ces matières, s'il avait connaissance de liens entre ces sociétés et les services de l'État, par exemple dans le cadre d'opérations de sous-traitance qui échapperaient ainsi au contrôle public. M. Urvoas m'a répondu par la négative, en ajoutant qu'il n'avait jamais rencontré les responsables de ces sociétés. Avez-vous des éléments d'information sur ce point ?

M. Jean-Marc Manach. Je n'ai pas de preuve d'une éventuelle utilisation, par les services, du système *Eagle* d'*Amesys* en Libye, au Maroc ou au Gabon ; en revanche, les services étaient bien entendu au courant des pratiques de cette société. On peut néanmoins s'étonner que le ministère des affaires étrangères, sous les mandats de Nicolas Sarkozy puis de François Hollande, ait gardé les mêmes éléments de langage, au mot près, pour dire qu'il n'avait pas à connaître de matériels grand public. Depuis décembre dernier, les systèmes de surveillance doivent être validés avant leur exportation : ce point a été ajouté à l'Arrangement de Wassenaar ; mais, entre-temps, *Amesys* a revendu son système *Eagle* à son chef de produit, lequel a créé une filiale domiciliée au Qatar – la maison mère d'*Amesys* étant, elle, restée à Boulogne-Billancourt. Que la France ait laissé faire me semble poser un vrai problème.

Quant à l'entreprise *Qosmos*, ses responsables prétendent que le matériel n'a jamais été livré, et rien ne prouve le contraire. J'ignore si un matériel a été expérimenté ; reste que cette société s'est, pendant des années, positionnée sur le marché de l'interception légale, avant de s'en retirer en octobre 2011 suite au scandale du projet *Asfador* en Syrie. J'ai réalisé, l'an dernier, une enquête sur *Qosmos* pour *Rue89*. Ses responsables m'ont confirmé que le retrait du marché signifiait la fin des ventes de la sonde à des entreprises comme *Utimaco*, prestataire en Syrie, ou *Amesys*, mais non les ventes entre les États eux-mêmes. Or *Qosmos* travaille avec les services – et pas seulement en France –, non dans le cadre d'une relation de sous-traitance, mais dans ses locaux mêmes. Je ne dispose pas de la liste complète des pays où la sonde a été vendue ; il y a quelques années, *Qosmo*s a ouvert une filiale à Singapour ; j'ignore ce qu'elle y fait. On évoque parfois un projet de contrat avec les Britanniques.

Dans une interview donnée au *Figaro*, un ancien salarié d'*Amesys* avait évoqué l'expérimentation, par la gendarmerie française, d'un système *Eagle* au Fort de Rosny, à des fins d'interception légale. Le DPI peut servir à des interceptions massives aussi bien que ciblées : je ne sais si la DGSE l'utilise pour identifier les courriels envoyés depuis une même adresse, par exemple. M. Delarue a parlé devant vous de numéros de téléphone, mais qu'en est-il de l'Internet et même des câbles sous-marins transatlantiques ? Sur ce point, le dernier

rapport de la délégation parlementaire au renseignement comporte des passages couverts d'astérisques. Il n'existe aucun cadre juridique en la matière. D'après un article de la revue *Intelligence online* paru l'an dernier, M. Urvoas, qui s'était entretenu avec M. Ayrault, M. Hollande et les responsables du renseignement du projet de loi de programmation militaire, se serait entendu répondre, s'agissant des câbles transatlantiques, que la question serait examinée plus tard. Ceux-ci sont-ils surveillés au niveau des points d'entrée ou de sortie ? Je l'ignore. La DGSE et la direction du renseignement militaire (DRM) ont, en France et à l'étranger, un certain nombre de stations d'écoute et d'interception des télécommunications par satellite ; j'en ai dressé la carte. Mais pour 90 % de communications, qui passent par les câbles, on ne sait à peu près rien, hormis ce qu'en a révélé Edward Snowden, en particulier pour le GCHQ. Celui-ci me semble davantage intéressé par les abonnés de la société *Orange* dans quelques pays à risques que par les abonnés français en France ; mais rappelons aussi que *France Télécom* contrôle 20 % des câbles transatlantiques au niveau mondial.

M. Edwy Plenel. Vos déclarations selon lesquelles *Qosmos* travaille avec la DGSE et la DGSI contredisent celles de M. Urvoas : les maintenez-vous ?

M. Jean-Marc Manach. C'est en tout cas ce que m'ont laissé entendre des personnes dignes de foi.

M. le coprésident Christian Paul. D'après ce que nous avions pu en savoir, la présence d'*Amesys* en Libye se faisait dans une grande proximité avec les autorités françaises.

M. Jean-Marc Manach. Il est avéré que le système *Eagle* a été développé en Libye par une entreprise française, et que Ziad Takieddine a touché des rétrocommissions illégales pour son rôle d'intermédiaire dans ce contrat. En revanche, on ne dispose pas de preuves que M. Guéant, M. Hortefeux et encore moins M. Sarkozy étaient informés du déploiement de ce système en Libye, même s'ils étaient informés – des échanges de courriers le prouvent – de l'existence de contrats.

Deux articles, respectivement parus dans *Le Canard enchaîné* et dans *Le Figaro*, laissent par ailleurs entendre que des membres des services de renseignement accompagnaient *Amesys* en Libye, ce dont on peut douter. Des personnes étaient au courant au sein des services, mais de là à conclure que ces derniers téléguidaient l'opération, il y a un pas que je ne franchirai pas. Au reste, *Amesys* a été plutôt lâchée dans la nature, contrairement à *Qosmos*.

M. le coprésident Christian Paul. S'agissant des interceptions entre la France et d'autres pays, n'y a-t-il pas un vide béant dans le contrôle des activités de renseignement, à commencer par celles qui visent nos propres compatriotes qui naviguent sur les millions de sites étrangers, y compris ceux mis en place par les opérateurs pour faire transiter les informations ?

M. Jean-Marc Manach. En Grande-Bretagne, les services de renseignement ont expliqué que le cadre juridique britannique ne pouvait s'appliquer aux citoyens qui utilisent des services de droit américain, tels que *Skype*, *Facebook ou Twitter*. Il faudra donc, dans la future loi, définir précisément le cadre juridique applicable à ceux de nos concitoyens qui utilisent, soit des services proposés par des entreprises étrangères, soit des serveurs étrangers. Comment la DGSE et la DGSI parviennent-elles à identifier les djihadistes en Syrie ou en Irak, sachant qu'ils communiquent plus souvent par Internet – *via* des entreprises étrangères – que par téléphone ? Mme Thatcher avait demandé aux services canadiens d'espionner certains

de ses ministres, qu'elle soupçonnait de déloyauté : il faut aussi se poser la question de la coopération entre les services.

M. le coprésident Christian Paul. Sur quels thèmes jugez-vous utile d'insister, s'agissant de la protection de la vie privée et des données personnelles ?

M. Jean-Marc Manach. Si la culture du renseignement fait défaut en France, c'est aussi parce que la « grande muette » ne communique pas. Cette position était tenable avant l'apparition d'Internet et éventuellement l'affaire Snowden, mais elle ne l'est plus désormais. L'absence de communication alimentera paranoïa et suspicion dans l'opinion. Les premières offres d'emploi mises en ligne par la DGSI concernaient des postes de webmaster : nous verrons bien si cela change quelque chose… Quant à la DGSE, son chargé de communication n'a accordé qu'une seule interview en plusieurs années. Lorsque Glenn Greenwald déclare, sur la foi d'une interprétation erronée, que la NSA espionne 70 millions de communications téléphoniques, cette dernière monte au créneau pour apporter un démenti. On ne peut imaginer une démocratie apaisée sans une communication qui dissipe les soupçons et les fantasmes : c'est au pouvoir politique qu'il incombe d'obliger les services à suivre cette voie, tout en renforçant les pouvoirs de la CNCIS.

M. le coprésident Christian Paul. Cette audition étant publique, j'espère que le message est passé.

M. Jean-Marc Manach. Sur Internet, on parle de vie sociale plutôt que de vie privée. Reste que, si l'État peut les y aider, c'est aux usagers eux-mêmes de protéger leur vie privée, par exemple en ouvrant l'onglet « navigation privée » du navigateur ou en chiffrant un courriel : cela permet aux avocats de protéger leurs clients et aux journalistes de protéger leurs sources. Cette culture de l'hygiène informatique doit faire partie du cursus de formation des professions concernées. Il a fallu attendre les années soixante-dix pour rendre le port de la ceinture de sécurité obligatoire dans les automobiles ; apparu dans les années soixante, Internet a pris son essor dans les années quatre-vingt-dix. Il est donc encore jeune, mais le temps est venu d'imposer des règles de sécurité. Contrairement à certaines idées reçues, chiffrer un courriel n'est pas difficile : il suffit de le vouloir.

La défense des libertés numériques est, au XXI^{e} siècle, ce que l'écologie était au XX^{e} : transpartisane, elle exige des actions immédiates, faute de quoi nous nous exposons à une évolution kafkaïenne, qui nous conduira à devoir prouver notre innocence si nous apparaissons comme suspect dans tel ou tel fichier. À Calais, des réfugiés figurant dans la base de données Eurodac en sont réduits à effacer leurs empreintes digitales pour ne pas être renvoyés en Grèce ou en Italie, où ils ont été fichés : *Minority report* est déjà une réalité. Si l'on ne remet pas l'humain au centre de la liberté numérique, le pire est à venir.

M. Edwy Plenel. La notion d'interception de sécurité telle que nous la définissons est déjà caduque, puisqu'il est question des usages numériques ou de la traçabilité. M. Delarue nous a tendu la main sur ce sujet.

M. Jean-Marc Manach. Je vous invite à réécouter l'audition d'Olivier Guérin, délégué général de la CNCIS, lors du colloque sur le renseignement organisé au Sénat il y a quelques mois. M. Guérin, dont je n'ai pu obtenir l'intervention écrite, évoquait des enregistreurs de mots de passe ou de frappe – « *keyloggers* » –, ou encore des balayages de port : autant de technologies hors du champ de la loi de 1991. Cela montre que la CNCIS est

déjà consciente que les pratiques des services en matière d'interception vont bien au-delà des écoutes téléphoniques.

Enfin, je veux évoquer la construction parallèle, que l'on a vu récemment apparaître aux États-Unis : si la NSA détient une information sur une vente de drogue à tel lieu et à telle heure, elle le fait savoir à la *Drug Enforcement Administration* (DEA), laquelle, comme par hasard, demande au FBI de faire un contrôle routier au moment et au lieu dits. De plus en plus souvent, et hors de toute légalité, la NSA est ainsi pourvoyeuse d'informations pour d'autres services. Je ne sais si le système existe en France, mais le fait est qu'il existe aux États-Unis.

M. le coprésident Christian Paul. Monsieur Manach, je vous remercie.

La séance est levée à onze heures quarante.