

ASSEMBLÉE NATIONALE

JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE

SESSION ORDINAIRE DE 2014-2015

217^e séance

Compte rendu intégral

2^e séance du mercredi 15 avril 2015

Les articles, amendements et annexes figurent dans le fascicule bleu ci-joint



<http://www.assemblee-nationale.fr>

SOMMAIRE

PRÉSIDENTE DE M. DAVID HABIB

1. Renseignement (p. 4173)

DISCUSSION DES ARTICLES (*suite*) (p. 4173)

Article 2 (*suite*) (p. 4173)

M. Sergio Coronado

Amendement n° 42 rectifié

M. Jean-Jacques Urvoas, rapporteur de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République

M. Jean-Yves Le Drian, ministre de la défense

Amendements n°s 20, 59, 283 rectifié, 21

Amendements n°s 184, 103 rectifié

M. Bernard Cazeneuve, ministre de l'intérieur

Amendements n°s 94, 145, 105 rectifié, 22, 23, 321, 24

Amendements n°s 25, 146, 185, 228, 259, 104, 26, 382, 437, 443 (sous-amendement), 441 (sous-amendement), 442 (sous-amendement), 147

Amendements n°s 284, 285, 27, 413

Amendements n°s 186, 28, 29, 187

Amendements n°s 357, 30, 188

Amendements n°s 358, 395, 380 deuxième rectification, 412 (sous-amendement), 148, 43, 149

Amendements n°s 44, 45, 46, 122, 189, 414, 190, 191, 192, 61, 69, 193

Article 3 (p. 4198)

M. Lionel Tardy

M. Jean-Jacques Candelier

Mme Isabelle Attard

M. Philippe Folliot

M. Jean Lassalle

M. Eduardo Rihan Cypel

M. Jean-Yves Le Drian, ministre

Amendement n° 152

Amendements n°s 126, 127, 194, 128

Amendements n°s 47, 129, 70, 137, 195, 132, 351 rectifié, 350, 32, 71, 196

Amendements n°s 341, 365, 342, 421

Mme Christiane Taubira, garde des sceaux, ministre de la justice

Amendements n°s 286, 327, 123, 48, 197, 383 (sous-amendement), 287

Après l'article 3 (p. 4204)

Amendement n° 314

M. Philippe Nauche, rapporteur pour avis de la commission de la défense nationale et des forces armées

2. Ordre du jour de la prochaine séance (p. 4204)

COMPTE RENDU INTÉGRAL

PRÉSIDENTE DE M. DAVID HABIB

vice-président

M. le président. La séance est ouverte.

(La séance est ouverte à vingt et une heures trente.)

1

RENSEIGNEMENT

Suite de la discussion d'un projet de loi

M. le président. L'ordre du jour appelle la suite de la discussion, après engagement de la procédure accélérée, du projet de loi relatif au renseignement (n^{os} 2669, 2697, 2691).

DISCUSSION DES ARTICLES *(suite)*

M. le président. Cet après-midi, l'Assemblée a commencé d'entendre les orateurs inscrits à l'article 2.

Article 2 *(suite)*

M. le président. La parole est à M. Sergio Coronado, dernier orateur inscrit sur l'article.

M. Sergio Coronado. Je souhaiterais replacer cet article dans l'économie globale du texte. J'avais dit, lors de la discussion générale, que ce projet de loi comportait essentiellement deux grands volets. Le premier vise à définir le périmètre de la communauté du renseignement, les finalités et les instances de contrôle. Nous en avons débattu. Des adaptations, des ouvertures ont été réalisées, le Gouvernement a pris en compte certains amendements des parlementaires. Chacun aura la possibilité d'évaluer si ces pas sont suffisants.

Le second volet, dont nous entamons maintenant l'examen avec l'article 2, autorise le recours à des dispositifs techniques de recueil de données de très grande ampleur, si ce n'est de masse. Ces dispositions ne sont pas tout à fait de la même nature. Autant il me semble que le premier volet est général et vise à être pérenne, autant les problèmes techniques liés à la surveillance, voire au contrôle, relèvent d'une autre nature.

Je rappelle que l'article 2 autorise, pour l'ensemble des finalités poursuivies par les activités de renseignement, la géolocalisation administrative en temps réel d'une personne, d'un véhicule ou d'un objet et l'utilisation en cours d'opération de dispositifs mobiles de proximité de captation directe de certaines métadonnées. Il permet également, pour les seuls besoins de la prévention du terrorisme, le

recueil en temps réel sur les réseaux des opérateurs de communications électroniques des données de connexion de personnes préalablement identifiées comme constituant une menace, voire, à titre exceptionnel, l'utilisation du dispositif des IMSI-catchers pour intercepter directement le contenu des correspondances. Il permet enfin, à des fins de prévention du terrorisme, l'exploitation par les opérateurs de communications électroniques et les fournisseurs de services des informations et documents traités par leur réseau, afin de révéler, sur la seule base de traitements automatisés d'éléments anonymes, une menace terroriste.

Je voudrais que tout soit bien clair, car beaucoup d'idées reçues viennent polluer nos débats. La première, on l'a vu hier au moment du rejet de l'amendement du Gouvernement, est que la radicalisation a lieu en prison. On ne dispose pas vraiment de données à ce sujet, et la garde des sceaux a donné des éléments hier montrant que ce n'était pas tout à fait vrai. Une autre idée reçue qui me paraît également extrêmement dangereuse consiste à dire que le recueil des métadonnées ne fait courir aucun risque car elles sont totalement anonymes. Certains collègues doutent peut-être du bien-fondé de mes critiques, mais ils doivent savoir que si j'avais accès ce soir à leurs données de connexion, j'en saurais sans doute davantage sur leur vie privée qu'après cinq ans à les côtoyer sur ces bancs. J'en saurais davantage sur leurs comportements, sur leurs habitudes alimentaires, sur leur orientation sexuelle, sur les gens qu'ils fréquentent, sans parler, comme l'a fait hier Isabelle Attard, de leurs passe-temps favoris la nuit venue!

M. le président. Nous en venons à l'examen des amendements à l'article 2.

La parole est à M. Sergio Coronado, pour soutenir l'amendement n^o 42 rectifié.

M. Sergio Coronado. Nous souhaitons, par cet amendement, revoir la définition des données de connexion donnée au nouvel article L. 851-1 du code de la sécurité intérieure, qui est issu de l'article 20 de la loi de programmation militaire. Nous ne souhaitons pas supprimer cet article 20, qui avait donné lieu à un grand débat extrêmement polémique à l'époque, notamment parce qu'il est très imprécis. Mais nous proposons d'harmoniser la rédaction de l'article L. 851-1 avec celle prévue au nouvel article L. 351-7, qui porte sur les dispositifs techniques de proximité. Nous l'avions déjà proposé lors des débats sur le projet de loi relatif à la géolocalisation. Le rapporteur nous avait demandé de retirer notre amendement en attendant le projet de loi sur le renseignement. Nous y voilà.

M. le président. La parole est à M. Jean-Jacques Urvoas, président et rapporteur de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, pour donner l'avis de la commission.

M. Jean-Jacques Urvoas, *rapporteur de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République.* La commission a repoussé cet

amendement, et pas seulement parce qu'il revient sur le débat sur l'article 20 de la loi de programmation militaire ! Il entend en effet encadrer le recueil des données de connexion *via* un dispositif technique dit « de proximité ». Or, en commission, ce dispositif a perdu sa qualification de « proximité » et, surtout, a fait l'objet d'un encadrement strict aux alinéas 23 et 24 du présent article, prenant ainsi en compte la préoccupation exprimée ici.

M. le président. La parole est à M. le ministre de la défense, pour donner l'avis du Gouvernement.

M. Jean-Yves Le Drian, ministre de la défense. Le Gouvernement est défavorable à cet amendement, qui a pour objet de limiter le champ des données de connexion accessibles aux services. Comme je l'ai dit, le périmètre des données de connexion accessibles est connu et précisément déterminé par des textes réglementaires depuis la loi du 23 janvier 2006. Il inclut les données permettant d'identifier l'utilisateur du terminal et celles relatives aux équipements, mais également aux dates, horaires et durées des communications, ou encore celles qui permettent d'identifier les destinataires de ces communications. Or, ces éléments sont évidemment extrêmement déterminants pour l'information des services. Il n'est donc pas question de revenir sur leur accessibilité.

M. le président. La parole est à Mme Laure de La Raudière.

Mme Laure de La Raudière. Je voudrais rappeler la demande d'explications qu'avait faite Christian Paul au Gouvernement à la fin de la séance de l'après-midi. D'autres d'entre nous avaient aussi posé de nombreuses questions qui n'ont pas eu de réponses.

Les questions essentielles, messieurs les ministres, sont de savoir en quel point du réseau de télécommunications vous entendez poser les sondes. Si c'est en cœur de réseau ou sur le routeur d'interconnexion, cela nécessite de recourir à un équipement supplémentaire si vous voulez aller au-delà de la loi actuellement en vigueur. Si vous voulez recueillir d'autres métadonnées que les données de connexion, vous serez obligé de mettre en place des équipements en cœur de réseau, des « *deep packet inspection* » : est-ce votre intention, ou pas ? Ces équipements, vous le savez, sont extrêmement intrusifs, puisqu'ils analysent l'ensemble des données qui circulent sur un réseau de télécommunications. Ils seront clairement le signe d'une surveillance de masse, ce dont, par ailleurs, vous nous avez dit ne pas vouloir.

Il paraît essentiel aujourd'hui, avant d'aller plus loin dans la discussion sur l'ensemble des amendements déposés à l'article 2, que vous nous éclairiez sur la façon dont vous allez procéder techniquement pour mettre en place vos sondes. Nous aurons ensuite d'autres questions sur les algorithmes. Je voulais rappeler cette demande, très sage, de Christian Paul.

M. le président. Je rappelle que nous en avons fini avec la discussion sur l'article...

(L'amendement n° 42 rectifié n'est pas adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 20.

M. Lionel Tardy. Cet amendement, de même que les n°s 21 et 22 qui viendront bientôt, concerne un problème que j'avais déjà identifié dans la loi de programmation militaire

et sur lequel vous remettez une couche. Il s'agit de l'article L. 246-1 du code de la sécurité intérieure, qui devient l'article L. 851-1.

Dans la liste que je vous ai citée tout à l'heure, il n'y avait que des données – je dis bien des données – pouvant être recueillies auprès des opérateurs. Alors qu'un an et demi s'est écoulé, je ne comprends pas pourquoi il est toujours question de recueil d'informations et de documents. Quels sont ces documents auxquels vous vous obstinez à faire référence ? À quel moment la loi autorise-t-elle le recueil de documents auprès des opérateurs ? Je ne vois pas de réponse. Je pense donc qu'il faut tout simplement supprimer cette référence, car il y a une suspicion que je souhaite lever, comme vous j'imagine, messieurs les ministres. La CNIL a formulé la même interrogation et estime que le périmètre est mal défini. Elle recommande de préciser la formulation, afin que seules les données de connexion – les données ! – puissent être recueillies. Tel est le sens de mes amendements n°s 20 à 22.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé cet amendement car nous avons déjà tenu ce débat sur l'article 20 du projet de loi de programmation militaire. M. Tardy avait d'ailleurs déjà exprimé un certain nombre d'incertitudes ou d'inquiétudes. Mais depuis, le décret du 24 décembre 2014 relatif à l'accès administratif aux données de connexion, codifié aux articles R. 246-1 et suivants du code de la sécurité intérieure, a apaisé toutes les craintes qui avaient été formulées. Nous considérons donc que l'amendement n'a pas lieu d'être.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Même avis.

(L'amendement n° 20 n'est pas adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 59.

M. Lionel Tardy. Je vous rassure, je n'ai pas l'intention de rouvrir le débat que nous avons eu lors de l'examen du projet de loi de programmation militaire. Ceci dit, vous apportez vous-même des modifications aux articles relatifs aux accès administratifs aux données de connexion. C'est donc l'occasion de revenir sur deux problèmes qui sont toujours, à mes yeux, irrésolus.

En effet, la liste des données pouvant être recueillies n'est pas exhaustive. Il est question de « recueil d'éléments », mais avec un « y compris » qui ne ferme pas la porte au recueil d'autres choses non mentionnées dans la loi. Je cite cette liste : données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électroniques, données relatives au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, données relatives à la localisation des équipements terminaux utilisés, données relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. Je propose de clore cette liste. L'accès administratif concerne les données que j'ai citées, mais rien ne nous garantit qu'il n'en concernera pas d'autres, sans que l'on sache lesquelles. C'est assez contradictoire, messieurs les ministres, avec votre volonté de définir un cadre légal.

(L'amendement n° 59, repoussé par la commission et le Gouvernement, n'est pas adopté.)

M. le président. La parole est à M. Jean-Jacques Urvoas, rapporteur, pour soutenir l'amendement n° 283 rectifié.

M. Jean-Jacques Urvoas, rapporteur. Je reprends en effet cet amendement en l'absence de ses signataires, car nous le trouvons pertinent. C'est une mesure de cohérence avec un amendement rédactionnel adopté tout à l'heure, qui vise à supprimer le terme « dûment ».

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Favorable.

(L'amendement n° 283 rectifié est adopté.)

M. le président. Monsieur Tardy, si je ne me trompe, vous avez déjà défendu l'amendement n° 21.

M. Lionel Tardy. Oui, monsieur le président.

(L'amendement n° 21, repoussé par la commission et le Gouvernement, n'est pas adopté.)

M. le président. Je suis saisi de deux amendements identiques, n°s 184 et 103 rectifié.

La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 184.

M. Sergio Coronado. Les alinéas 10 à 16 introduisent deux innovations extrêmement importantes : le recueil en temps réel sur les réseaux d'opérateurs de données et, surtout, la possibilité de mettre en place des algorithmes avec le nouvel article 851-4 du code de la sécurité intérieure, qui est une disposition contestée par un nombre très important de citoyens et d'acteurs du numérique. Vous connaissez le principe, puisqu'il a été expliqué lors des travaux de la commission : on fait dériver l'ensemble du trafic d'un hébergeur qui centralise des milliards de données vers une boîte noire, on applique à ces données des algorithmes qui auront été paramétrés préalablement et on observe ce qui remonte de ce grand coup de filet.

Certains ont comparé la méthode à de la pêche au chalut, ou au filet maillant dérivant ; il reste qu'elle suppose le recueil d'un nombre très important de données et que, contrairement à ce qu'on a pu entendre en commission, elle concerne l'ensemble du trafic. Les algorithmes permettent par définition, et même par nature, la surveillance de masse, puisque c'est l'ensemble de nos données qui est pris dans le filet et passé au crible de l'analyse.

Je rappelle également, je l'avais dit au Premier ministre lors des questions au Gouvernement mardi, que l'ensemble des hébergeurs français se sont inquiétés de ces dispositifs, en particulier de leur impact économique. D'après le rapporteur, l'algorithme, sur lequel personne n'aura de visibilité d'ailleurs, compte tenu de sa classification, opérera sur la seule base des métadonnées. Si l'on considère que les métadonnées sont les données de navigation, le seul moyen de les obtenir auprès d'un fournisseur d'accès, qui ne les voit pas passer en clair, est de mettre en place, comme l'a rappelé Mme de La Raudière voilà quelques instants, des dispositifs d'analyse de trafic de type *deep packet inspection*, ou DPI, qui consistent à analyser le contenu de chaque paquet IP transitant par un équipement sur lequel un dispositif d'analyse est opérant. Par voie de conséquence, lorsque ce dispositif est installé au niveau d'un équipement majeur tel qu'un cœur de réseau, il permet d'opérer une surveillance généralisée de l'ensemble du trafic des abonnés.

Je rappellerai pour conclure que, voilà quelques mois, dans le cadre de l'examen du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, vous aviez jugé, monsieur le ministre, qu'une telle solution était particulièrement intrusive,...

Mme Laure de La Raudière. Ne pouvez-vous pas faire autrement, monsieur le ministre ?

M. Sergio Coronado. ...qu'elle présentait des risques importants en matière de sécurité des réseaux compte tenu de l'absence de visibilité des opérateurs et qu'elle était particulièrement onéreuse : près de 150 millions d'euros par an, sur la base des éléments que vous aviez vous-même fournis. Je vous renvoie au compte rendu de ces débats.

M. le président. La parole est à Mme Laure de La Raudière, pour soutenir l'amendement n° 103 rectifié.

Mme Laure de La Raudière. Il est identique. Je ne reposerai pas encore une fois mes questions au sujet des sondes, monsieur le ministre, mais nous souhaiterions vraiment obtenir une réponse, un éclairage de votre part. Nous attendons que vous nous rassuriez sur le fait que vous n'utiliserez pas le DPI. Mais si vous n'utilisez pas une telle technique, que vous avez jugée trop intrusive, qu'en sera-t-il pour les sondes ?

Pour en rester à ces fameux algorithmes qui permettront de détecter de potentiels djihadistes, êtes-vous bien certains qu'ils sont efficaces ? Pour ma part, j'en doute : d'après les chercheurs en intelligence artificielle et les experts de ce type d'algorithmes, cet outil ne serait pas efficace. Par ailleurs, quel que soit le type d'algorithmes choisis, la surveillance sera massive. Cette méthode revient à détecter des cas rares dans une base de données très large, c'est-à-dire à chercher une aiguille dans une meule de foin. Il est en particulier très difficile de repérer des vrais suspects. Avec cette méthode, vous identifieriez de nombreux « faux positifs » et demanderez ainsi la levée de l'anonymat et la mise sous surveillance de beaucoup de personnes totalement innocentes.

Quel type d'algorithmes allez-vous utiliser ? Comment allez-vous procéder ? Quels résultats espérez-vous obtenir ?

M. le président. Quel est l'avis de la commission sur ces deux amendements identiques ?

M. Jean-Jacques Urvoas, rapporteur. Ces amendements proposent de supprimer les deux dispositifs innovants de cet article. Parce qu'ils seront suivis de plusieurs autres sur le sujet, je propose au ministre que nous prenions le temps de nous y arrêter, de donner l'essentiel de nos arguments afin que nos collègues soient parfaitement éclairés et puissent ainsi progresser dans leur réflexion.

Sur le plan strictement technique, monsieur Coronado, l'article L. 851-3 ne procède pas de la police judiciaire. Il n'y a donc pas lieu d'établir des comparaisons avec les moyens judiciaires, comme vous le faites dans l'exposé sommaire de votre amendement, car l'article renvoie à une activité de police administrative.

Quant à l'article L. 851-4, concernant le fameux algorithme, la volonté exprimée par le Gouvernement n'est pas celle d'une collecte massive, d'un traitement généralisé de données, puisqu'il n'y a de captation que dans le cas où une menace est détectée. Et, si j'ai bien compris, le suivi est renforcé.

L'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 qui est évoqué ne me paraît pas pertinent non plus. Nous reviendrons par la suite à ce fameux arrêt *Digital Rights Ireland*. D'une part, il concerne non pas les États mais les opérateurs privés, et je ne suis pas certain qu'il faille immédiatement en tirer des conséquences pour l'État, et d'autre part il n'est pas pertinent de s'y référer ici puisque l'article L. 851-4 ne propose pas une surveillance de masse.

Enfin, M. Coronado pointe dans son exposé sommaire le caractère illusoire de l'anonymat des données de connexion. C'est la raison pour laquelle la notion de levée d'anonymat a été supprimée du texte adopté par la commission, au profit de celle d'identification, utilisée uniquement dans des cas bien circonscrits. La présidente de la Commission nationale de l'informatique et des libertés – CNIL – nous en avait convaincus.

La commission a donc émis un avis défavorable sur ces deux amendements.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Ainsi que vient de l'indiquer le rapporteur, nous entrons dans le débat sur l'essentiel des techniques utilisées. Je vais développer mon sentiment sur la question assez longuement, afin d'éclairer la suite de nos discussions.

Les amendements qui viennent d'être défendus visent à supprimer deux mesures importantes du projet de loi : la surveillance renforcée d'individus présentant une menace terroriste particulière et la détection de telles menaces grâce au jeu d'algorithmes permettant de révéler des comportements de communication suspects, deux dispositions auxquelles le Gouvernement est nécessairement favorable. Permettez-moi toutefois d'y revenir pour éclairer notre point de vue sur les amendements qui viendront ensuite en discussion et clarifier le débat.

Le premier mécanisme d'accès aux données de connexion, tout en suivant une logique de ciblage individuel, agit sur l'ampleur des données collectées et le caractère instantané de l'accès.

M. Lionel Tardy. Non ! Ce n'est pas possible !

M. Jean-Yves Le Drian, ministre. L'article L. 851-3 permet ainsi aux services d'accéder en continu à l'ensemble des données de connexion d'un certain nombre de personnes identifiées comme possiblement engagées dans des réseaux ou des projets terroristes. La surveillance est donc exercée en temps réel et porte sur l'exhaustivité des données de connexion. Il s'agit toutefois bien de données de connexion, et non pas de contenu.

Mme Isabelle Attard. C'est pire !

M. Jean-Yves Le Drian, ministre. La procédure d'autorisation pour chacune des personnes surveillées est celle de droit commun : autorisation du Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement. Le contrôle est précisé : il revient à la CNCTR, et au juge si ce dernier est saisi. La finalité est uniquement la prévention du terrorisme.

J'en viens à présent aux algorithmes, sujet sur lequel vous me permettrez d'être un peu plus long. Ce mécanisme répond, comme l'ont relevé les observateurs, à une nouvelle logique : la surveillance ne porte pas sur des cibles préalablement et nominativement identifiées, mais procède

de manière ciblée – ciblée, j'insiste – à la surveillance des modes de communication spécifiques utilisés par les terroristes. C'est indispensable pour repérer des réseaux que nous ne connaissons pas avant qu'ils n'agissent.

L'article L. 851-4 permet ainsi au Premier ministre d'imposer aux opérateurs et aux prestataires de services d'installer sur leurs réseaux, et donc sur les flux de données de connexion qu'ils traitent, des traitements automatisés, également qualifiés d'algorithmes, qui repèrent non pas des personnes pré-identifiées mais des comportements de communication suspects en termes de risque terroriste.

M. Lionel Tardy. Cela ne marche pas !

M. Jean-Yves Le Drian, ministre. Ces traitements permettent dans un second temps, et après une seconde autorisation, d'identifier des personnes à surveiller. Il n'est donc question ni de surveillance de masse ni de captation et de stockage de la totalité des données transitant sur le réseau. Il s'agit bien plutôt d'un ciblage, portant non pas sur des individus mais sur des modes de communication que les services auront pu identifier comme étant caractéristiques de l'activité de personnes impliquées dans l'action terroriste.

En effet, ces dernières n'échangent pas ou plus vraiment par mail ou par téléphone sur leurs projets : elles utilisent pour communiquer des procédés clandestins en s'appuyant, sur internet, sur des outils spécifiques ou détournés de leur usage originel. Par ailleurs, elles font évoluer très fréquemment leurs modes de communication. Ce sont ces procédés qui, une fois repérés, permettent la conception d'algorithmes destinés à détecter des personnes susceptibles d'être impliquées dans le terrorisme.

Ce n'est d'ailleurs que dans un second temps que, le cas échéant, et toujours sous contrôle de la CNCTR, les services pourront accéder à l'identité des personnes ainsi détectées.

Je vais vous donner un exemple significatif, qui a déjà été cité en commission : si Daech met en ligne une vidéo de décapitation sur des sites djihadistes connus, puis se connecte sur d'autres sites pour s'assurer de la bonne réception et de la bonne qualité des images et du message, cette dernière activité se traduit par des connexions à certaines heures, depuis certains lieux, sur certains sites. Un algorithme permet de trier anonymement les connexions et de repérer ainsi un trafic caractéristique.

M. Lionel Tardy. Si je me connecte pour voir une vidéo de Daech, alors je suis concerné ?

M. Jean-Yves Le Drian, ministre. Je pourrais vous citer des cas que j'ai moi-même suivis en tant que ministre de la défense, et qui démontrent l'importance de ce dispositif.

Sachez en outre que le texte apporte des garanties majeures, puisque les résultats de ces traitements seront soumis au groupement interministériel de contrôle – GIC, service du Premier ministre qui a vocation à les centraliser sous l'autorité de ce dernier ; ils ne seront donc pas directement transmis au service concerné, ce qui est un point essentiel. La méthode de mise en œuvre des traitements sera en outre négociée avec les opérateurs ou les prestataires concernés en fonction des situations et des besoins.

Les garanties apportées par le texte sont les suivantes. Premièrement, seule la finalité de prévention de terrorisme justifie l'usage de ces dispositifs, et c'est la CNCTR qui le valide. Deuxièmement, les opérations ne portent que sur des données de connexion. Troisièmement, elles sont réalisées

sous le pilotage et le contrôle du GIC. Quatrièmement, la méthode utilisée pour la détection ainsi que le périmètre de la recherche sur les réseaux seront définis et soumis au préalable à la Commission. Toute opération de recueil et toute modification de l'algorithme devront faire l'objet d'une autorisation au cas par cas. Cinquièmement, la Commission pourra contrôler en permanence le dispositif, ses évolutions, les traitements réalisés et les résultats obtenus. Sixièmement, seules les données nécessaires à la détection des alertes seront collectées. Septièmement, les services ne pourront accéder aux données autres que le résultat du traitement. Ils n'auront donc directement accès ni aux banques de données des opérateurs ni à leurs flux globaux. Huitièmement, ils ne pourront avoir accès à l'identité des personnes éventuellement concernées que sur une seconde autorisation expresse du Premier ministre prise après l'avis de la CNCTR.

Les amendements adoptés en commission sur l'initiative du président rapporteur ont permis de préciser, d'explicitier l'ensemble de ces garanties et le Gouvernement l'en remercie.

Le Gouvernement a en outre été sensible aux préoccupations exprimées par les hébergeurs, auxquels il a été fait référence tout à l'heure. Ils ont fait part de leurs observations sur le texte dans une lettre adressée récemment au Premier ministre. Ce matin, le ministre de l'intérieur, le ministre de l'économie et la secrétaire d'État au numérique ont rencontré leurs représentants.

Un accord important me paraît avoir été trouvé, et monsieur le ministre de l'intérieur pourra utilement compléter mon propos dans quelques instants. Il porte tout d'abord sur la compréhension des objectifs du Gouvernement, que je viens d'énumérer, ensuite sur la méthode qui sera suivie dans la mise en œuvre des dispositions de l'article L. 851-4, et enfin sur les éléments à renforcer dans la rédaction de cet article. Le Gouvernement déposera à cette fin plusieurs amendements.

Ces amendements, qui viendront tout à l'heure en discussion, apportent de nouvelles garanties. Premièrement, ils rappellent que le principe de proportionnalité s'applique. Deuxièmement, en application directe de ce principe, ils exigent du Premier ministre qu'il indique le périmètre des données de connexion sur lesquelles l'algorithme sera appliqué. Troisièmement, ils garantissent aux opérateurs que ce sont leurs propres agents qui installeront sur leurs réseaux les dispositifs prévus à l'article L. 242-9 du code de la sécurité intérieure, qui devient l'article L. 861-3. Quatrièmement, ils excluent tout recours au régime d'urgence pour cette technique. Enfin, ils limitent à quatre mois renouvelables la durée de l'autorisation du Premier ministre et, comme l'a annoncé ce dernier dans sa présentation du texte, limitent également la durée de vie de cette nouvelle technique au 31 décembre 2018, son renouvellement étant subordonné aux conclusions de l'évaluation qui en sera faite en termes d'utilité et de proportionnalité.

Tels sont les éléments de garantie et de clarté que nous souhaitons apporter au sujet de cette technologie. Si nous souhaitons la mettre en œuvre, c'est qu'elle est indispensable pour nous protéger contre les menaces terroristes qui sont en train de s'organiser, dont je pourrais donner de nombreux exemples.

M. le président. La parole est à Mme Isabelle Attard.

Mme Isabelle Attard. Permettez-moi de céder à la mode du « vrai-faux » qui semble sévir au sein du Gouvernement sur ce projet de loi.

Vous nous dites, monsieur le ministre de la défense, que les données de connexion sont moins importantes, ou en tout cas moins précises, que le contenu lui-même. C'est faux ! Et malheureusement pour vous, nous ne sommes pas les seuls à le dire. Quiconque s'y connaît un tout petit peu en informatique pourrait vous le confirmer.

M. Lionel Tardy. Évidemment !

Mme Isabelle Attard. Comme je l'ai démontré hier soir, les informations obtenues sont encore plus riches lorsqu'elles sont assorties de métadonnées et de données de connexion, puisque l'on peut alors savoir avec qui la personne est en relation tant de fois par jour ou par semaine, combien de temps dure la conversation, quels sont les conversations menées et les sites consultés ultérieurement. Ainsi, les données sont encore plus précieuses. C'est bien pourquoi elles sont au centre des préoccupations des géants mondiaux de l'informatique.

Vous nous dites ensuite que ces fameux algorithmes pourront détecter des comportements suspects. C'est encore faux ! Les comportements sont différents à chaque attaque terroriste !

M. Lionel Tardy. Bien sûr !

Mme Isabelle Attard. Dès lors, que mettez-vous dans l'algorithme ? Sans oublier qu'il ne s'agit pas d'une formule magique pondue par un ordinateur : ce sont des humains qui créent et qui gèrent ces algorithmes. À tout moment, ce sont des humains qui donnent les consignes et entrent les mots clés.

Les comportements terroristes changent donc en permanence.

M. Jean-Yves Le Drian, ministre. Justement !

M. Lionel Tardy. Que faites-vous lorsque les terroristes cryptent leurs données, monsieur le ministre ?

Mme Isabelle Attard. Ce ne sont pas des tours que l'on a attaqués au mois de janvier, mais une rédaction. Techniquement, donc, comment vous y prenez-vous ? J'attends votre réponse. Ne vous inquiétez pas, nous avons encore toute la soirée. (*Exclamations sur les bancs du groupe SRC.*) Mes chers collègues, je crois que le sujet est suffisamment important pour que l'on en discute !

M. le président. Madame Attard, vous avez épuisé votre temps de parole dans quelques secondes...

Mme Isabelle Attard. Vous nous dites enfin qu'il ne s'agit pas de surveillance de masse. Pour une fois, vous avez raison : il ne s'agit pas de surveillance de masse, il s'agit de surveillance généralisée. C'est bien pire !

J'espère en tout cas, mes chers collègues, que vous avez pu lire pendant la pause l'excellent article d'Andréa Fradin dans *L'Obs*, qui explique à quel point les algorithmes seront inutiles.

M. le président. La parole est à M. Guillaume Larrivé.

M. Guillaume Larrivé. Messieurs les ministres, mes chers collègues, de quoi parlons-nous ? D'une guerre, celle que nous a déclarée un ennemi islamiste radical, armé, qui veut détruire par la terreur la plus barbare nos sociétés démocratiques.

Au nom de qui parlons-nous ? Nous parlons au nom du peuple français. Notre devoir, pardonnez-moi de le dire de façon un peu grave et solennelle, est de nous efforcer de définir une sorte de bouclier numérique destiné à mieux protéger les Français. Y parviendrons-nous ? Je l'espère. En tout cas, nous avons le devoir d'y travailler.

Plus nous avançons dans le débat et plus j'écoute les arguments des quelques députés qui défendent ces amendements de suppression, plus je suis convaincu de l'impérieuse nécessité de voter le dispositif proposé par les autorités exécutives. Oui, pour une finalité unique et précisément définie, celle de la lutte contre le terrorisme, nous devons donner à ces grands services publics que sont les services de renseignement des moyens technologiques nouveaux, en l'espèce un algorithme qui permettra d'identifier des comportements constituant de véritables menaces nationales.

Et nous le faisons en ayant chevillée au corps, au cœur et à l'esprit la nécessité d'exercer certains contrôles démocratiques. Nous avons passé une partie de l'après-midi à renforcer de manière consensuelle l'organisation, les compétences et les modalités d'intervention de la Commission nationale de contrôle des techniques de renseignement. Sera-t-elle compétente pour contrôler l'algorithme ? Oui, pleinement et de manière renforcée !

En outre, le dispositif n'entrera en vigueur, si nous le votons, que pour trois années, période au terme de laquelle la représentation nationale en réalisera l'évaluation.

Ce dispositif, je le voterai, et j'avoue ne pas comprendre les raisons pour lesquelles certains s'obstinent encore à le combattre.

M. le président. La parole est à Mme Laure de La Raudière.

Mme Laure de La Raudière. Rassurez-vous, monsieur Larrivé : je ne le combats pas, je souhaite simplement obtenir des réponses à mes questions. Ce système est-il efficace ou ne l'est-il pas ? Quelles sont les évaluations réalisées à ce sujet, sachant que l'on ne trouve rien dans l'étude d'impact ? Conduit-il ou non à une surveillance massive ?

M. Lionel Tardy. J'ajouterai : quel est son coût ?

Mme Laure de La Raudière. Sur tous ces points, je ne suis pas éclairée. Or notre rôle de députés est d'éclairer le peuple français sur ces questions majeures.

Après votre exposé, monsieur le ministre de la défense, je n'arrive toujours pas à comprendre comment les choses se passeront concrètement. Je suis vraiment désolée d'entrer dans les aspects techniques, mais c'est le seul moyen de savoir s'il s'agira ou non d'une captation généralisée de données. Lorsque l'on parle d'outils numériques, on ne peut s'affranchir de ce passage par la technique.

Monsieur le ministre, y aura-t-il utilisation de DPI dans le cœur de réseau ? Si tel n'est pas le cas, c'est que vous procéderez autrement : en utilisant quelles techniques ? S'agira-t-il de captation de données aux extrémités, par exemple uniquement chez les hébergeurs ? Merci de nous renseigner ! Nous voulons vraiment avancer dans le débat. Il nous faut comprendre ce que vous allez faire, précisément pour nous déterminer sur le vote de cet article.

M. le président. La parole est à M. Lionel Tardy.

M. Lionel Tardy. Faisons un peu de technique. En dehors de ma fonction de député, il se trouve que c'est mon métier, alors j'en profite !

Encore une fois, tout ce que vous dites est parfaitement défendable, monsieur le ministre de la défense. Il faut en effet trouver des solutions. Hélas, nous butons sur la technique. Cela a déjà été le cas pour la loi HADOPI : nous savons tous que ce texte n'a strictement rien donné. Parmi ceux qui s'adonnaient au téléchargement illégal, beaucoup ont mis en place des VPN, des réseaux privés virtuels : maintenant, la HADOPI peut toujours courir après !

Il faut donc parler technique, je suis désolé. Vous pourrez faire tout ce que vous voulez sur le plan politique, le sujet restera technique.

M. Bernard Cazeneuve, ministre de l'intérieur. Vous n'êtes pas le seul à le maîtriser, monsieur Tardy, ne vous inquiétez pas !

M. Lionel Tardy. Nous allons donc parler technique toute la soirée, monsieur le ministre. Je ne m'inquiète pas : je le répète, il se trouve que c'est mon métier.

Nous l'avons vu hier, vous justifiez votre programme de surveillance de masse par une analogie avec l'analyse de données commerciales, en faisant mine, au passage, d'oublier que les autorités étatiques sont dotées de pouvoirs autrement plus intrusifs que celui de nous envoyer les publicités ciblées qui peuplent nos boîtes de *spam*.

Lorsque l'on recourt à l'analyse de données pour repérer des cas d'usurpation d'identité ou de fraude bancaire à la carte de crédit, on se fonde sur des modèles construits annuellement à partir de plusieurs milliers d'exemples connus. Or le terrorisme ne présente pas d'indices statistiques similaires. Autrement dit, le phénomène ne présente pas la fréquence nécessaire pour en extraire un modèle significatif. Comment construire un algorithme à partir de cela ? D'autant qu'il y a très peu de chances pour que les attentats de demain présentent les mêmes méthodes opérationnelles que ceux d'hier.

Alors que les méthodes automatisées de détection préventive procèdent, pour leur traitement du futur, par induction à partir d'un passé connu, le principe de ces actions asymétriques est au contraire la surprise, la non-reproduction des scénarios répertoriés. Comme le résume le juriste américain Jeffrey Rosen, c'est donc vouloir « chercher une aiguille dans une botte de foin alors que la couleur et la forme de l'aiguille ne cessent de changer ».

Même en supposant que le terrorisme présente des signatures repérables par analyse de données, ce qui est pour le moins hasardeux, pareil système va engendrer pléthore de suspects, dont une écrasante majorité de fausses pistes, et ceci par millions.

Bref, je vous souhaite bonne chance pour analyser toutes ces données et pour prouver la validité de votre information.

M. le président. La parole est à M. Pascal Popelin.

M. Pascal Popelin. J'avoue en toute humilité que la technique n'est pas mon métier. J'essaie néanmoins de procéder avec logique. J'ai écouté avec attention les exemples que Mme Attard nous a produits hier soir pour démontrer combien les métadonnées pouvaient être parlantes. Mais, pour qu'elles le soient, il faut les recouper et les interpréter. Si les services ne faisaient que tout recueillir

– à supposer qu'ils en aient les moyens – ils perdraient leur temps. En outre, ils auraient un bien piètre algorithme, puisqu'il est précisé que les données analysées sont uniquement celles qui sont liées à la lutte contre le terrorisme. L'exemple du club échangiste pris par Mme Attard s'inscrit-il vraiment dans ce cadre? Si les services faisaient entrer de telles données dans l'algorithme, on pourrait légitimement penser qu'ils sont très mauvais, et douter aussi que la CNCTR valide le processus! Et, comme dans tous les autres cas cités par notre collègue, ils se placeraient de toute façon dans l'illégalité car leur action serait contraire aux finalités de la loi.

Il n'y a donc pas de surveillance de masse, d'abord parce que c'est humainement impossible, ensuite parce que c'est inefficace au regard de ce qui motive le recours à ce type d'outil, enfin et surtout parce que c'est contraire à ce texte. C'est d'ailleurs ce qui lui donne toute sa force du point de vue des libertés individuelles.

M. le président. La parole est à M. Éric Ciotti.

M. Éric Ciotti. Nous sommes face à un débat technique, nous disent des experts. Bien sûr.

Mme Laure de La Raudière. Mais non, ce n'est pas que cela!

M. Éric Ciotti. Cependant, l'honneur de notre assemblée est aussi d'exprimer notre attachement à des valeurs et de livrer un combat pour la démocratie, la République, la protection des libertés, en nous fondant sur des convictions politiques. Le débat doit être technique, certes, mais il doit être également politique, ce qui nous ramène à l'objet même de ce projet de loi: la lutte contre le terrorisme.

Avec plusieurs collègues, j'ai visité ce matin place Beauvau l'unité de coordination de la lutte antiterroriste, l'UCLAT, et sa plate-forme téléphonique de signalement des appels au djihad. Le chef de cette unité nous a remis à cette occasion un document en anglais, en accès quasi libre sur internet, qui recense les « bonnes pratiques » du terroriste en Occident.

Je ne suis pas un expert, je le concède bien volontiers à ceux qui le sont. Néanmoins, je pense que nous devons nous pourvoir d'outils techniques de protection contre le terrorisme et je fais confiance aux spécialistes de nos services, dont l'expertise est reconnue, pour les mettre en place.

Certains invoquent divers risques ou menaces auxquels le dispositif nous exposerait. Je ne partage pas leur point de vue. Nous sommes ici au cœur de la lutte contre le terrorisme. Que l'on cesse de dire que cela sera techniquement inefficace: quand bien même on n'arriverait à détecter qu'un seul comportement à risque, à éviter un seul attentat, nous aurions fait œuvre utile! Soutenons le dispositif et arrêtons donc de soulever des menaces en permanence! Ce ne sont pas ces techniques qui menacent les libertés, ce sont ceux qui brandissent l'arme du terrorisme contre les libertés.

M. Guillaume Larrivé. Très bien!

M. le président. Je vais maintenant donner la parole à M. Christian Paul, qui l'a demandée. Le ministre et le rapporteur ont tous deux souligné l'importance de ces deux amendements, ce qui explique que j'aie dérogé au règlement en laissant intervenir plusieurs orateurs. Mais après cette intervention et la réponse du ministre de l'intérieur, nous passerons au vote.

M. Christian Paul. Il est en effet nécessaire et souhaitable que cet échange ait lieu, d'autant que nous n'avons pu débattre en fin de séance tout à l'heure et obtenir des réponses avant de passer à l'examen des amendements.

Nous sommes devant une affaire de la plus haute importance. Il est rare que le *New York Times* consacre son éditorial à la France, et la dernière fois, c'était sur ce texte! Ce seul fait, sans juger du contenu de l'article, appelle une discussion approfondie au sein de notre hémicycle. Comme d'autres l'ont dit avant moi, nous sommes strictement dans notre rôle de parlementaires. Nous ne cherchons pas à soulever les peurs et les comportements irrationnels, comme a pu le faire M. Larrivé, avec son esprit habituel de croisade, ou comme M. Ciotti s'y emploie de façon permanente.

M. Guillaume Larrivé. Chef de la fronde, vous voilà arbitre des élégances!

M. Christian Paul. Il faut regarder les faits!

M. le ministre de la défense s'est livré à un gros effort d'explication, ce qui était important dans ce débat. Comme souvent, deux objectifs que nous partageons tous, la sécurité des Français et la préservation de leur liberté, entrent en tension. Il faut trouver la façon de gérer cette tension, particulièrement vive à propos de ce texte.

Pour faire avancer le débat, je souhaite vous faire part de deux interrogations. Monsieur le ministre de la défense, vous avez parlé de la captation – le choix des termes n'est pas aisé et peut-être conviendrait-il de parler plutôt de collecte, de traitement – en temps réel de l'exhaustivité des données de connexion.

M. le président. Monsieur le député, il est temps de conclure.

M. Christian Paul. Monsieur le président, je n'ai pas abusé de mon temps de parole sur les amendements précédents. La capture de ces données est-elle exhaustive lorsqu'il s'agit d'un traitement qui ne s'inscrit pas dans le temps et n'appelle pas le stockage? Dans ce cas, il convient de le préciser.

Cela m'amène à une deuxième remarque: j'ai la conviction, depuis le début du débat en commission des lois, que le seul cadre que l'on ait voulu se donner est la finalité des opérations – la lutte contre le terrorisme – et, bien sûr, le passage par la commission de contrôle, sur lequel il nous faudra revenir.

M. le président. Veuillez conclure.

M. Christian Paul. Nous n'avons pas suffisamment encadré de façon normative la nature des documents concernés et les activités de traitement. Nous devons le faire davantage, sans quoi la brèche qui aura été pratiquée à l'occasion de ce texte sera considérable.

M. le président. La parole est à M. le ministre de l'intérieur.

M. Bernard Cazeneuve, *ministre de l'intérieur.* Je veux remercier l'ensemble des intervenants, quelle que soit leur position. J'essaierai de leur apporter des éléments de réponse pour ce qui concerne le ministère dont j'ai la responsabilité, en complément de ce que vient de dire excellemment le ministre de la défense.

Pour commencer, il y a, dans le débat public, une bonne part d'hypocrisie. Les opérateurs internet détiennent nos données personnelles et je suis convaincu que nombre

d'entre eux utilisent des techniques extraordinairement intrusives à l'égard de nos propres existences. Ainsi, M. Facebook vous demande si vous êtes prêt à être ami avec des tas de personnes dont vous ne lui avez jamais indiqué que vous les connaissiez. J'aimerais savoir comment M. Facebook parvient à le savoir!

Vous pouvez secouer la tête, madame Attard, forte de votre compétence et de votre assurance, mais les responsables de l'entreprise m'ont bien dit, lorsque je me suis rendu dans la Silicon Valley, qu'ils utilisaient ces techniques. Ils seront à Paris le 20 avril, car nous entretenons une relation de confiance dans le but de bâtir ensemble une politique intelligente de prévention du terrorisme.

Bref, les opérateurs ont accès à nos données personnelles, et nul ne sait dans cet hémicycle ce qu'ils en font. Mais cela n'indigne personne. Cela ne pose aucun problème lorsqu'il s'agit de grands trusts internationaux, dont je m'empresse de dire que certains ont délocalisé leurs bases fiscales, puissants et suffisamment organisés pour parvenir à convaincre des parlementaires d'intervenir sur un certain nombre de sujets – qu'ils alimentent d'ailleurs de leurs connaissances techniques, en leur expliquant qu'il y a ceux qui savent et ceux qui ne savent pas. Mais lorsqu'un État se propose de prévenir le terrorisme sur internet, il est nécessairement suspect de poursuivre des objectifs indignes! Eh bien moi, je n'adhère pas à cela. (*Applaudissements sur de nombreux bancs du groupe SRC et du groupe UMP.*)

M. Sébastien Denaja. Très bien!

M. Bernard Cazeneuve, ministre. Il y a, dans cette présentation des choses, une forme de soumission, à tout le moins de faiblesse, à l'égard des grands groupes que pour ma part je n'accepte pas. Je suis républicain et j'estime que lorsqu'un État se propose de mobiliser des moyens pour lutter contre le terrorisme, il n'a pas à être suspecté, surtout par les mêmes qui considèrent qu'il est tout à fait normal et logique que ces groupes utilisent nos données personnelles sans aucun contrôle – un contrôle que, d'ailleurs, personne ne réclame. Je n'ai pas la même approche.

Il est un autre point sur lequel je voudrais insister : on ne peut répéter à l'envi des choses fausses, ni considérer, madame Attard, que sous prétexte que c'est écrit dans le journal, c'est vrai. J'ai appris à l'école à ne pas croire ce qu'il y a dans les journaux ou dans les livres, à exercer mon esprit critique et user de ma libre conscience plutôt que de gober béatement et benoîtement ce que dit la presse. Moi, ce qu'il y a dans les articles de presse, par principe je ne le crois pas. Je suis un esprit libre et indépendant et j'entends le demeurer. Bref, c'était peut-être dans *L'Obs*, ou dans le *Petit Bessin illustré*, mais par nature, et par essence, je n'y crois pas.

Enfin, monsieur Tardy, vous répétez sans cesse qu'il y aura une surveillance de masse, que nous allons entrer dans les données et dans les conversations, que ce sera *Big Brother*. Eh bien moi, je vais créer un hashtag : #NiBigNiBrother! Je suis tout à fait légitime à le faire et je vais vous dire pourquoi.

Nous avons expliqué le fonctionnement des deux techniques que vous mettez en cause et leur finalité.

Mme Laure de La Raudière. Ce n'est pas vrai!

M. Bernard Cazeneuve, ministre. Si. Et vous, monsieur Tardy, vous niez de la tête avant même que l'on vous réponde. Vous prenez la parole pour expliquer que le sujet

est suffisamment technique pour justifier d'une réponse du Gouvernement, et quand on vous la donne, avec précision et sincérité, vous regardez tout cela avec un incommensurable mépris. Ce comportement est injustifiable!

Deux techniques sont donc en cause : le suivi en continu des terroristes et la détection sur données anonymes. Elles sont selon vous extraordinairement intrusives et permettent de prélever en masse des données. C'est faux. Avec M. Le Drian, nous avons expliqué pourquoi à maintes reprises ; je vais m'y employer une nouvelle fois.

La première technique consiste à essayer d'obtenir des données de connexion sur des listes préétablies de personnes : c'est donc le contraire du prélèvement de données en masse. Ces personnes sont connues pour présenter un risque terroriste particulièrement élevé. Selon vous, le fait de procéder, par des mesures de police administrative portant sur une liste bien définie de personnes, à la prévention de la commission d'un acte terroriste relève-t-il d'une surveillance de masse? Ces dispositifs sont placés sous le contrôle de la CNCTR, du juge administratif et éventuellement du juge pénal, s'ils sont mobilisés en contravention avec les règles du droit! À tout moment, la CNCTR peut vérifier qu'il y a bien conformité entre la technique et les individus ciblés, qui sont considérés comme présentant un risque terroriste majeur!

Bien que ces explications aient été données, au Parlement et devant l'opinion publique, il est des parlementaires qui continuent à considérer qu'il vaut mieux ne rien faire, et laisser ces terroristes agir, plutôt que de mobiliser ces techniques. Sous prétexte que seul le juge judiciaire est compétent pour traiter de ces questions, il vaut mieux intervenir une fois les actes commis, dans le cadre d'une procédure judiciaire! Ce n'est en aucun cas l'approche du ministre de l'intérieur, en charge de la protection des Français.

S'agissant de la détection sur données anonymes, je voudrais citer des cas très concrets auxquels j'ai été confronté dans mes fonctions de ministre de l'intérieur – car la lutte contre le terrorisme amène aussi une expérience, une compétence, un vécu.

Mes services de renseignement ont pu, par des échanges d'informations, savoir que des terroristes procédaient, sur le darknet, à des communications cryptées donnant des éléments précis sur leur intention de commettre des actes terroristes. Par ailleurs, on sait que, et cela a été le cas dans les attentats du mois de janvier, des terroristes utilisent, pour poster des vidéos appelant au terrorisme et faisant la publicité d'actes terroristes qu'ils ont déjà commis, une multitude d'adresses IP qui se masquent les unes les autres, à partir de messages postés depuis différentes boîtes situées partout sur la planète. En tant que ministre de l'intérieur, chargé donc de prévenir la survenue d'actes de terrorisme, lorsque mes services, dont la haute compétence, monsieur Tardy, est reconnue de ceux qui, au Parlement et dans l'exécutif, ont la charge de les contrôler ou d'en assurer la direction, m'ont dit qu'il était possible, grâce à des algorithmes, de détecter des comportements et d'identifier des individus susceptibles de passer à l'acte, eh bien oui, j'ai souhaité utiliser en toute transparence ces techniques!

Il ne s'agit pas de techniques de prélèvement de masse, non, c'est faux! Ce sont au contraire des techniques de ciblage. C'est précisément parce que nous ne voulons pas de ce prélèvement de masse, que nous nous l'interdisons, que nous faisons toute la lumière sur ces techniques. Nous utilisons ces formules mathématiques pour prendre seule-

ment ce dont nous avons besoin sur le flux. En l'occurrence, ce n'est pas le contenu des conversations qui nous intéresse, mais les données de connexion.

Si nous sommes amenés à vouloir disposer du contenu des conversations, nous sommes obligés de repasser devant la CNCTR. Si elle considère que nous ne sommes pas légitimes à le faire, elle peut saisir le juge administratif. Si le juge administratif considère qu'en l'ayant fait, nous avons commis une infraction pénale, il peut saisir le juge judiciaire.

Il est mensonger de dire que ces techniques visent à prélever massivement des données. Il est mensonger de dire que cela se fait sans contrôle. Il est mensonger de dire que le juge n'intervient pas. Mais je constate que, face à des lobbies puissants, qui ont la possibilité de diffuser de nombreux messages sur internet, une vérité peut être, pendant un temps, plus faible qu'un agglomérat de mensonges.

Face au terrorisme, au risque qu'il représente, la vérité implique que nous soyons rigoureux et que nous expliquions ce que nous faisons, et ce sous votre contrôle, celui de la CNCTR et celui du juge.

Compte tenu de la menace qui pèse sur le pays, de la gravité de ce qui peut advenir, je suis exaspéré de voir que, sur un sujet aussi grave, à propos duquel nous nous appliquons à apporter, dans la plus grande des sincérités, le maximum de précisions, il puisse y avoir autant d'amalgames, autant d'approximations et, parfois, autant d'arrogance! (*Applaudissements sur de nombreux bancs des groupes SRC et UMP.*)

(Les amendements identiques n° 184 et 103 rectifié ne sont pas adoptés.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 94.

M. Lionel Tardy. Il est défendu.

(L'amendement n° 94, repoussé par la commission et le Gouvernement, n'est pas adopté.)

M. le président. La parole est à M. Jean-Jacques Candelier, pour soutenir l'amendement n° 145.

M. Jean-Jacques Candelier. Le nouvel article L. 851-3 du code de la sécurité intérieure permet, s'agissant des seuls besoins de la lutte antiterroriste, et pour certaines personnes présentant un risque en matière de terrorisme, un accès instantané en temps réel aux données de connexion, c'est-à-dire aux réseaux des opérateurs.

Certes, le contenu même de ces échanges est exclu : seule une interception de sécurité permettra d'y accéder. Pour autant, le périmètre des données pouvant être recueillies est très large. Il s'agit en effet, selon la lettre du futur article L. 851-1 du code, « des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. »

Or, comme le souligne parfaitement le Syndicat de la magistrature, le glissement de la sollicitation *a posteriori* auprès des opérateurs vers la ponction directe sur les réseaux est d'autant plus préoccupant que les critères sont peu restrictifs. Il n'est en effet requis aucun risque imminent d'action terroriste pour mettre en œuvre cette modalité dérogatoire de recueil. C'est la raison pour laquelle nous proposons cet amendement qui limite ce dispositif dérogatoire aux cas de menace terroriste imminente.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé cet amendement, qui rendrait le dispositif inopérant.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Défavorable.

(L'amendement n° 145, repoussé par le Gouvernement, n'est pas adopté.)

M. le président. La parole est à Mme Laure de La Raudière, pour soutenir l'amendement n° 105 rectifié.

Mme Laure de La Raudière. Il tend à préciser que ce sont bien les données de connexion que vous voulez récupérer, monsieur le ministre.

Je suis désolée si je donne l'impression de dire des mensonges, parce que ce n'est pas du tout mon objectif. En revanche, je serais rassurée si vous me précisiez la méthode par laquelle vous allez procéder. Allez-vous utiliser la technique du *deep packet inspection* pour recueillir les données ? Dites-le nous simplement, cela nous rassurerait. Expliquez-nous juste ça.

Je n'ai vraiment pas envie de mentir, le sujet est beaucoup trop grave, et vous avez parfaitement raison d'essayer de mobiliser l'ensemble des moyens pour lutter contre le terrorisme. Mais reconnaissez aussi que nous avons le droit, connaissant certaines technologies intrusives, de vous poser des questions. Des questions qui pour l'instant, n'ont pas reçu de réponse.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Pour m'en tenir strictement à l'amendement de Mme de La Raudière, il se présente presque de manière rédactionnelle mais tend en réalité à remettre en cause la lettre de l'article 20 de la loi de programmation militaire. Avis défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Madame de La Raudière, nous avons déjà échangé sur cette question, je ne sais pas si vous vous en souvenez.

Mme Laure de La Raudière. Oh oui !

M. Bernard Cazeneuve, ministre. Lorsque nous discutons de la loi du 13 novembre 2014 et que nous évoquons la question du blocage administratif des sites, vous m'aviez déjà demandé si nous utilisions la technique du DPI. J'avais alors déclaré devant l'Assemblée nationale qu'il était hors de question d'utiliser cette technique, et je le confirme.

Mme Laure de La Raudière. C'était pour du filtrage internet, ce n'est pas pareil.

M. Bernard Cazeneuve, ministre. Je vous confirme ce que j'ai dit de façon inlassable depuis des jours et des semaines – mais à peine la réponse est-elle donnée qu'elle est oubliée, et il faut y revenir; ce n'est pas vous que je vise en l'occurrence, madame de La Raudière, mais plutôt le brouhaha ambiant et le vacarme médiatique. Nous n'utiliserons pas cette technique. C'est très clair. Je l'ai déjà dit au mois de novembre et je le répète aujourd'hui. Nous avons un processus très encadré qui consiste à prendre les données de connexion d'un groupe ciblé, d'où l'utilisation de la détection sur données anonymes. Si nous voulons entrer dans les communications, la procédure nous oblige à redemander l'autorisation à la CNCTR, et cette demande doit être fortement motivée. Nous n'utiliserons donc en aucun cas cette technique du DPI.

M. le président. La parole est à Mme Isabelle Attard.

Mme Isabelle Attard. Monsieur le ministre, sachez qu'il est extrêmement choquant d'être considérée comme non-républicaine, selon vos propos, tout simplement parce que j'essaie d'être constructive et de vous dire, comme nous l'avons fait avec Laure de La Raudière sur le projet de loi terrorisme, ce qui marchera ou ne marchera pas.

Sachez, et je l'ai répété plusieurs fois depuis lundi soir, que nous sommes tous concernés par la lutte contre le terrorisme. Nous cherchons à trouver des solutions qui marchent et à engager les moyens financiers et humains de notre pays dans des méthodes qui vont donner des résultats.

Aujourd'hui même, le patron de la NSA a reconnu sous serment que les écoutes généralisées n'avaient permis de ne déjouer qu'un seul attentat, et encore. Au début, il avait annoncé un chiffre de cent, mais sous serment, il a avoué que cela ne concernait qu'un seul attentat.

M. Sébastien Denaja. C'est déjà bien !

Mme Isabelle Attard. Excusez-moi de revenir là-dessus, monsieur le ministre: vous m'avez interpellée sur les données personnelles collectées...

M. le président. Merci de conclure, madame Attard.

Mme Isabelle Attard. Je vais faire vite, mais lorsque l'on est qualifiée de non-républicaine alors que l'on essaie de défendre les libertés individuelles tout en étant efficace, c'est extrêmement gênant. Je n'ai pas fait de rappel au règlement, mais j'aurais très bien pu. (*Exclamations sur les bancs du groupe SRC.*)

Mme Sylvie Tolmont. On n'a pas dit non-républicaine, mais arrogante !

Mme Isabelle Attard. Vous parlez donc, monsieur le ministre, des données personnelles utilisées par Facebook: j'espère que tout le monde entend bien que Facebook est un service, et qu'il a donc accès à toutes les données de son service! Si je ne veux pas mettre mes données sur Facebook, je ne les mets pas. Et beaucoup de Français ne sont pas sur les réseaux sociaux pour cette raison. C'est un choix de leur part. Il n'y a pas de surveillance généralisée de la part de Facebook, c'est un choix que d'y aller!

Vous nous dites que cette collecte n'émeut personne, mais cela émeut beaucoup de monde. J'ai déposé des questions écrites, nous en avons parlé, j'ai posé des questions orales au Gouvernement sur Amazon. Et j'étais toute seule à le faire.

Monsieur le ministre, si le syndicat Alliance Police nationale dénonce aujourd'hui ce projet de loi, c'est parce qu'il demande des moyens. Il mendie pour avoir quelques voitures, afin que les renseignements territoriaux puissent faire leur travail de détection des comportements à risque sur notre territoire!

M. Sébastien Denaja. Votez le budget avec nous en ce cas !

M. le président. Madame Attard...

Mme Isabelle Attard. La lutte contre le terrorisme, c'est peut-être 60 000 agents de plus et des moyens financiers!

M. le président. Merci Mme Attard. Je vous ai laissé dépasser largement le temps qui vous était imparti. La parole est à M. le ministre.

M. Bernard Cazeneuve, ministre. Madame Attard, je suis désolé, mais il semble que vous ne soyez guère au courant des débats sur le budget du ministère de l'intérieur – peut-être n'était-ce pas dans *Le Nouvel Observateur* ? Si vous y aviez participé, vous sauriez ce qui a été voté. Il est exaspérant de vous entendre dire des choses qui, une fois de plus, ne correspondent pas à la réalité.

Je vais vous apporter la démonstration que ce que vous dites est très loin de la réalité. Nous avons décidé, avec le Premier ministre, d'augmenter significativement les moyens du renseignement territorial et de la police. Nous avons créé 432 postes depuis le début du quinquennat au sein de la direction générale de la sécurité intérieure. Nous avons augmenté son budget de 12 millions d'euros par an. Le Premier ministre a décidé de créer 500 postes en trois ans au sein du renseignement territorial. Dans le budget 2014, pour la première fois depuis des années, nous allouons 4 000 véhicules aux forces de l'ordre, soit un budget de 40 millions d'euros par force au cours des années 2014 et 2015 qui a été voté par la représentation nationale. Nous créons près de 100 postes au sein de la direction centrale de la police judiciaire pour la lutte contre le terrorisme et le fonctionnement de la plateforme Pharos. Nous créons 500 au sein de la direction générale de la sécurité intérieure, en plus des 432 que j'ai déjà cités. Nous créons également 100 postes de plus au sein de la direction du renseignement de la préfecture de police de Paris.

Alors quand vous vous avancez sur des sujets que visiblement vous ne connaissez pas, comme je viens d'en apporter la démonstration, faites-le au moins sans arrogance. Cela a l'air de vous amuser, mais ça ne fait pas rire les policiers, pas davantage que lorsqu'ils vous entendent théoriser à longueur de temps les violences policières. Croyez-moi, compte tenu des violences dont ils sont eux-mêmes victimes, ça les indignes. Alors permettez-moi de vous dire que ce discours et cette démagogie sont inacceptables sur des sujets aussi sérieux. (*Applaudissements sur plusieurs bancs des groupes SRC et UMP.*)

(*L'amendement n° 105 rectifié n'est pas adopté.*)

M. le président. Monsieur Tardy, il me semble que vous avez déjà présenté l'amendement n° 22.

M. Lionel Tardy. Oui, monsieur le président.

(*L'amendement n° 22, repoussé par la commission et le Gouvernement, n'est pas adopté.*)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 23.

M. Lionel Tardy. Nous allons sans doute nous focaliser sur les boîtes noires dans les amendements suivants, mais il ne faut pas négliger les autres techniques autorisées, qui méritent tout autant d'être étudiées à la loupe. Ici, il est question du recueil en temps réel sur le réseau. Je m'étais interrogé sur la notion de sollicitation du réseau lors de la discussion de la loi de programmation militaire : je ne comprenais pas ce que cela voulait dire. En fait, cela signifie visiblement que l'on sollicite les opérateurs pour recueillir des données.

Aujourd'hui, je regrette cette notion qui disparaît du texte que vous nous proposez. En effet, c'est une évolution majeure, comme le note la CNIL, puisque les services de renseignement, donc l'État, peuvent aspirer des données directement sur le réseau. Cela ne me rassure pas du tout, d'autant moins que je lis dans l'avis de la CNIL – ce n'est pas *Le Nouvel Observateur* – que c'est « de nature à permettre l'aspiration massive et directe des données par les agents (...), par l'intermédiaire de la pose de sondes. »

Il s'agit d'une vraie nouveauté et de vrais risques d'intrusion. La seule garantie, et je la salue, est que seule la lutte contre le terrorisme pourra justifier cela. Mais on verra que dans le texte, il y a encore six autres sujets qui sont très différents.

Cependant, je pense qu'il faut rétablir le principe de subsidiarité et passer par les opérateurs, ne serait-ce que pour des raisons philosophiques, relatives au rôle de l'État, et des raisons techniques. Il faut absolument rétablir le principe d'une sollicitation des opérateurs. C'est une garantie petite, mais nécessaire.

Cet amendement a donc pour objet de rajouter que ce recueil en temps réel se fait par l'intermédiaire des opérateurs. La formulation n'est sans doute pas optimale, mais vous avez parfaitement compris l'objectif de cet amendement qui tend à éviter une aspiration directe et massive par l'État qui risque fort de ne pas concerner que des terroristes, loin de là.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Je suis désolé mais la commission a repoussé cet amendement. Tout d'abord, il n'a pas grand-chose à voir avec le principe de subsidiarité, contrairement à ce qui est écrit dans son exposé sommaire. Surtout, la mention proposée pourrait sembler minorer le rôle que le Premier ministre doit tenir dans l'organisation du dispositif.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Défavorable.

(L'amendement n° 23, repoussé par le Gouvernement, n'est pas adopté.)

M. le président. La parole est à M. Jean-Jacques Urvoas, pour soutenir l'amendement n° 321.

M. Jean-Jacques Urvoas, rapporteur. Il s'agit d'un amendement de précision.

(L'amendement n° 321, accepté par le Gouvernement, est adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 24.

M. Lionel Tardy. Il s'agit d'un simple amendement de précision. Nous étions partis du principe que toute mise en œuvre se faisait sur autorisation du Premier ministre. Ici, les termes employés sont « sous le contrôle du Premier ministre », ce qui n'est pas tout à fait la même chose. Pour être totalement clair, je pense donc qu'il faut bien écrire qu'il s'agit d'un régime d'autorisation.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable. Cet amendement est satisfait sur le fond, puisque l'autorisation qui est mentionnée à l'alinéa 12 fait nécessairement référence à une décision du Premier ministre, qui est en charge de toutes les autorisations de la présente loi. En outre, en supprimant le mot « contrôle », l'adoption de cet amendement pourrait paradoxalement amoindrir le rôle du Premier ministre dans la mise en œuvre des dispositions prévues.

(L'amendement n° 24, repoussé par le Gouvernement, n'est pas adopté.)

M. le président. Je suis saisi de cinq amendements identiques, n° 25, 146, 185, 228 et 259.

La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 25.

M. Lionel Tardy. Avec les boîtes noires, nous arrivons à l'un des points... noirs du texte. Franchement, je ne sais pas par où commencer, et je n'aurai sans doute pas assez de deux minutes. Je vais donc faire une liste des raisons qui me conduisent à demander leur suppression.

Premièrement, elles posent un problème philosophique. Comme l'a souligné le Conseil national du numérique – qu'il faudrait écouter de temps en temps – s'en remettre à un algorithme est un choix de société douteux. Cela peut convenir pour chercher ses vacances, mais je ne vois pas l'intérêt pour cibler des terroristes.

Ensuite, on ne connaît pas la localisation de ces sondes : seront-elles aux cœurs de réseau ou aux points d'interconnexion qui ne voient pas passer l'intégralité du trafic ? Ce serait alors peu efficace pour le trafic échangé localement entre cellules terroristes. Ou bien seront-elles au plus proche des abonnés finaux ? Dans ce cas, cela impliquerait d'aller reconfigurer plus de 50 000 équipements.

On ne connaît pas non plus le périmètre des métadonnées. Seules les adresses IP seront-elles concernées, ou également les adresses des contenus ? C'est une vraie question, car les dernières, sans doute les plus pertinentes, ne figurent pas dans les métadonnées traitées par les fournisseurs d'accès. Le droit national et communautaire leur interdit de procéder au traitement et à la conservation des données de trafic. Le seul moyen de les obtenir serait de mettre en place des dispositifs d'analyse de trafic de type DPI, très intrusifs. Toutefois, le ministre de l'intérieur n'était pas du tout pour une telle solution lors de l'examen de la loi sur le terrorisme, car cela engendrerait effectivement une surveillance généralisée.

Quatrièmement, l'étude d'impact est très légère, voire muette sur ces points, mais aussi sur le coût de toutes ces mesures – nous y reviendrons tout à l'heure – et les modalités de compensation des intermédiaires.

Enfin, encore une fois, même si seule la lutte contre le terrorisme est concernée, le caractère potentiellement intrusif de ces dispositions reste particulièrement élevé. Je sais que

vous proposez une durée de quatre mois renouvelables. Toutefois, le problème n'est pas la durée, mais bien la technique et son contrôle.

Pour toutes les raisons que j'ai évoquées et que je viens de détailler, une adoption de ce dispositif nuirait aux libertés individuelles et aux acteurs du numérique. Peut-être, monsieur le ministre, pouvez-vous nous rappeler les modalités d'utilisation des DPI.

M. le président. La parole est à M. Jean-Jacques Candelier, pour soutenir l'amendement n° 146.

M. Jean-Jacques Candelier. Défendu.

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 185.

M. Sergio Coronado. Je tiens à réagir au ton qu'ont soudainement pris nos débats. On observe parfois, de la part des parlementaires, y compris de ma part, des maladroites, des abus ou même des postures. Mais entendre dire, lorsqu'un parlementaire conteste certaines dispositions du projet de loi, qu'il n'est pas patriote, qu'il n'est pas républicain, qu'il fait preuve de démagogie... Ce n'est pas une façon de mener le débat ! Nous pouvons discuter calmement, même quand il y a un désaccord. Quand nous posons des questions, comme souvent au cours de cette soirée, il faut essayer d'y répondre. Je ne prétends pas être technicien, et je refuse d'ailleurs de l'être : nous sommes parlementaires, nous légiférons au nom du peuple, dans l'intérêt général, et les questions que nous posons sont légitimes...

Mme Laure de La Raudière. Bien sûr !

M. Sergio Coronado. ...même quand elles peuvent paraître bêtes.

Fils de prof, je sais que la pédagogie consiste à répéter, répéter et répéter encore, à vouloir toujours expliquer et convaincre. Vous le savez aussi, monsieur le ministre – on ne devient pas ministre sans être capable de faire preuve de pédagogie à tout moment, même quand on est un peu irrité. Il conviendrait de retrouver la tonalité qui était celle de nos débats avant cet incident, afin que nos débats jusqu'à une heure du matin restent apaisés et argumentés.

Comme un certain nombre de nos collègues donc, nous proposons de supprimer les alinéas 14 à 16. Comme je l'ai dit tout à l'heure, l'article L. 851-4 du code de la sécurité intérieure ouvre la possibilité, à des fins de prévention du terrorisme, d'une collecte de grande ampleur – je n'utiliserai pas les mots qui fâchent, comme « massive » ou « généralisée » – et d'un traitement des données.

Le fait que cette surveillance porte initialement sur des données ne permettant pas l'identification d'une personne, traitées de façon automatique et algorithmique, ne saurait être une garantie suffisante : c'est le sens de l'avis qu'a rendu la commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, à laquelle certains d'entre nous, délégués par leur groupe, appartiennent. Cet argument est d'ailleurs traditionnellement avancé à l'appui de la surveillance généralisée, qui a recours à des algorithmes qui lisent et exploitent des volumes massifs de données.

M. le président. La parole est à M. Christian Paul, pour soutenir l'amendement n° 228.

M. Christian Paul. Sur ce sujet, il n'y a pas de passion sans bonne raison. S'il y a de la passion, c'est parce que la menace terroriste existe, qu'elle est extrêmement inquiétante et réitérée. Il n'en demeure pas moins que ce texte a été conçu avant les attentats les plus récents, comme on nous l'a dit à plusieurs reprises : il s'inscrit donc dans une réflexion de longue durée.

S'il y a de la passion, c'est aussi parce que, sur ces questions, une grande démocratie a failli. Les révélations que l'on relie un peu rapidement à l'affaire Snowden, mais dont certaines se sont produites avant ou après, ont montré qu'une grande démocratie pouvait faillir. Ce n'est pas la nôtre, mais c'est une démocratie qui a une longue histoire, une longue tradition et qui dispose de juristes, de contrôles, de règlements et d'un Parlement. À un moment donné, cette démocratie a probablement laissé se déployer un certain nombre de pratiques qui ont été heureusement dénoncées depuis.

S'agissant des grandes plates-formes, monsieur le ministre de l'intérieur, nous n'en sommes pas au soldé de tout compte. Heureusement, un règlement sur les données personnelles est en cours de préparation par la Commission européenne, car la question de la loyauté des plates-formes comme Google ou Facebook est essentielle. Nous n'en avons pas fini avec les géants du capitalisme informationnel : ce n'est même que le début. Il faudra mettre en place une régulation – c'est un autre sujet, mais je tiens à l'évoquer car il est important de l'avoir à l'esprit.

L'amendement que je présente, avec plusieurs de mes collègues du groupe SRC, notamment Patrick Bloche...

M. Lionel Tardy. On ne l'entend pas souvent !

M. Christian Paul. ...et Martine Martinel, ici présents, vise à supprimer les alinéas 14 à 16. À ce moment du débat, j'ai le sentiment qu'un certain nombre de questions ont été posées. Je répète ce que j'ai dit tout à l'heure : l'exhaustivité des données traitées...

M. le président. Merci de conclure, monsieur Paul...

M. Christian Paul. C'est une question essentielle, monsieur le président !

M. le président. Monsieur Paul, vous vous exprimez depuis deux minutes trente !

M. Christian Paul. Je veux bien, mais sur un sujet comme celui-là...

M. le président. Ce n'est pas à vous de décider, monsieur Paul.

M. Christian Paul. Dans ce cas, monsieur le président, j'arrête là ! Je ne motiverai pas davantage mon amendement !

M. le président. Excusez-moi de vous le rappeler, mais il y a un règlement et ma responsabilité est de l'appliquer.

M. Christian Paul. C'est insupportable !

M. le président. La parole est à M. Philippe Noguès, pour soutenir l'amendement n° 259.

M. Philippe Noguès. Je vais essayer de prendre le relais : les dispositifs dont parlait Christian Paul, similaires aux techniques de surveillance qui furent illégalement employées par la NSA, légalisent en effet une pratique de surveillance non ciblée, utilisant des matériels et logiciels fonctionnant sur la base d'algorithmes pour filtrer l'ensemble des données circu-

lant sur les réseaux. L'article 2 ouvre ainsi la possibilité d'analyser l'ensemble des communications électroniques au niveau d'un réseau ou d'un serveur, et donc de mettre en place un traitement massif des données personnelles de l'ensemble des citoyens sans aucun motif précis.

S'agissant des conditions de recours à cette technique de surveillance, la CNCTR n'aura qu'un simple avis à donner pour qu'il soit permis, pour une durée de trente jours renouvelables sans limitation. La prévention contre le terrorisme étant une mission récurrente des services de renseignement, cette mesure pourra être utilisée de façon quasi-permanente.

Par ailleurs, la garantie de l'anonymat n'est absolument pas assurée. Certes, le texte précise que seul le Premier ministre pourra lever l'anonymat en cas de menace avérée, mais les professionnels d'internet rappellent que la combinaison d'un petit nombre de données suffit à identifier des personnes, démontrant le caractère illusoire de cette protection.

M. le président. Quel est l'avis de la commission sur ces amendements identiques ?

M. Jean-Jacques Urvoas, rapporteur. Naturellement, la commission a repoussé tous les amendements visant à supprimer les alinéas concernés, pour deux raisons essentielles.

Nous légiférons aujourd'hui en nous inspirant de la loi de 1991, qui a été écrite, comme cela a déjà été beaucoup dit, à une époque où ni internet ni le téléphone portable n'existaient. Pourtant, cette loi est encore appliquée et elle rend les services que chacun s'accorde à lui reconnaître. Si cette loi a été forte, c'est parce qu'elle n'a pas été écrite en fonction d'une finalité.

Il est important qu'une loi prévoie les modalités de contrôle des mécanismes qu'elle invente. Or la commission des lois a veillé scrupuleusement à renforcer partout les mécanismes de contrôle. Quand le Gouvernement a proposé cet algorithme, il n'était pas encadré aussi sérieusement que nous le souhaitons : avec l'accord du Gouvernement, nous avons donc adopté des amendements visant à ce que la CNCTR, dont nous avons passé beaucoup de temps cet après-midi à renforcer la composition et qui est aujourd'hui consensuelle au sein de l'Assemblée nationale, ait accès en permanence à cet algorithme. Si ce dernier devait évoluer, la CNCTR le saurait. C'est elle qui donne des autorisations.

Il est évident que la responsabilité est assumée par les pouvoirs publics, et singulièrement par les services du Premier ministre. Il ne peut en être autrement : puisqu'il s'agit d'un outil de l'État, l'État doit en assumer la responsabilité, comme les ministres ne cessent de le dire.

Parce que nous estimons que les conditions d'un contrôle effectif sont réunies, aussi bien vis-à-vis de l'outil existant que de son évolution éventuelle, la commission souhaite que l'article 2 du projet de loi comporte les alinéas 14 à 16. En conséquence, la commission est défavorable à tous les amendements visant à les supprimer.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Dans le souci de garantir la sérénité de nos débats, je veux répondre à M. Coronado avant qu'il ne parte – il n'est pas naturel qu'il siège tellement à droite dans cet hémicycle !

M. Éric Ciotti. Nous lui avons accordé l'asile ! (*Sourires.*)

M. Sergio Coronado. J'attendais justement votre réponse, monsieur le ministre !

M. Bernard Cazeneuve, ministre. Il n'y a en effet aucune raison de considérer que ceux qui ne pensent pas comme nous ne sont pas républicains. Par conséquent, vous avez aussi toutes les raisons de penser qu'il n'y a pas, d'un côté, des parlementaires soucieux des droits de l'homme et de l'autre, un Gouvernement et des services de renseignement qui voudraient tous les jours les remettre en cause. Vous avez aussi raison de considérer que la politique est un art de la pédagogie. Mais, pour participer à des débats parfois compliqués, je sais que la politique partage cela avec la mauvaise foi, qui, pour être efficace, doit aussi être constamment répétée et réitérée.

Je veux redire à tous les parlementaires qui affirment que la technique que nous mobilisons est une technique de masse, comme M. Noguès à l'instant, que j'ai apporté il n'y a pas dix minutes des réponses extrêmement précises sur ce sujet. J'ai expliqué en quoi ce n'était pas le cas, comment le dispositif était ciblé et quels étaient les outils de contrôle. Si nous n'avons pas été suffisamment clairs, nous pouvons réexpliquer les choses.

En tout cas, nous avons apporté ces explications et conçu ces dispositions avec la plus grande sincérité. Nous pouvons le considérer en toute bonne foi, au moins entre nous : si nous prenons autant de temps pour expliquer une mesure qui ne concerne que la lutte contre le terrorisme, c'est tout simplement parce que nous sommes déterminés à ce qu'il n'y ait pas le moindre décalage entre les dispositions de la loi, l'esprit dans lequel elle a été écrite, les intentions du Gouvernement et les faits qui suivront l'application de la loi, c'est-à-dire la politique mise en œuvre par le Gouvernement dans ce domaine.

M. le président. La parole est à Mme Isabelle Attard.

Mme Isabelle Attard. Monsieur le ministre, si nous souhaitons que les alinéas 14 à 16 soient supprimés, c'est parce qu'ils contiennent les dispositions que nous refusons dans ce projet de loi. Tout le reste nous convient, avec quelques aménagements – la commission a d'ailleurs amélioré grandement ce texte.

Pourquoi considérez-vous donc, monsieur le ministre, que je fais preuve d'arrogance ? Ce n'est pas de l'arrogance, mais de l'inquiétude, et la volonté farouche de lutter avec vous, par tous les moyens, afin de déjouer les attentats en préparation. Je ne mets nullement en cause les services de renseignement.

M. Jean-Jacques Urvoas, rapporteur. Ah bon ?

Mme Isabelle Attard. Bien au contraire : je souhaite qu'ils aient le plus de moyens efficaces possibles pour lutter contre le terrorisme.

M. Jean-Yves Le Drian, ministre. Eh bien voilà !

Mme Isabelle Attard. C'est bien de cela que nous parlons : des moyens efficaces, utiles, dont le fonctionnement ne remet pas en cause les libertés les plus fondamentales, parmi lesquelles le droit au respect de la vie privée.

Lionel Tardy parlait tout à l'heure de détecter une aiguille dans une botte de foin. Pour trouver ce qu'ils cherchent, les algorithmes et les boîtes noires que vous vous apprêtez à mettre en place ont bien besoin de tout regarder, avant de cibler. Ce n'est pas en grossissant la taille de la botte de foin

que l'on va aider les services de renseignement. Les algorithmes, ces fameuses formules, ces recettes de cuisine, fonctionnent selon des critères définis par les humains et sur la base de données relatives aux précédents attentats, de façon à pouvoir déjouer les attentats en préparation. Mais ils ne sont jamais les mêmes ! Pour reprendre l'image de M. Tardy, ce n'est pas la couleur de l'aiguille qui va changer dans la botte de foin, puisque tous les attentats sont différents et que les procédés et les méthodes seront toujours différents, mais la forme même de l'objet que l'on est en train de chercher. Aujourd'hui, c'est une aiguille : demain, ce sera un caméléon, et après-demain, une fourchette.

M. le président. La parole est à M. Lionel Tardy.

M. Lionel Tardy. Monsieur le ministre, j'aimerais que vous nous éclairiez un peu plus sur ces boîtes noires.

M. Jean-Jacques Urvoas, *rapporteur* et **M. Jean-Yves Le Drian**, *ministre* Elles ne s'appellent pas « boîtes noires » !

M. Lionel Tardy. On a l'impression que la boîte noire est un petit équipement. Or, du côté des hébergeurs et des opérateurs, si on veut analyser en temps réel des flux sans effet sur leur vitesse, ce sont des armoires complètes, des équipements très sophistiqués qu'il faudra installer !

D'un point de vue technique, il faudra que des personnes extérieures puissent intervenir chez les opérateurs : vous m'expliquerez comment cela se passera en termes de sécurité. Généralement, les *data centers* font partie des équipements les plus sécurisés actuellement... Comment va-t-on permettre à une personne extérieure d'accéder à ces fameuses boîtes noires, à ces armoires noires ? Cela pose de vraies questions.

Ces boîtes noires permettront l'écoute à tout instant de tout trafic d'un hébergeur ou d'un fournisseur d'accès à internet dans le but de rechercher de potentiels terroristes. Comme je l'ai déjà dit, il s'agit pour moi d'une mesure vaine parce que les personnes visées savent utiliser les réseaux anonymes, comme Tor ou VPN, pour chiffrer leurs connexions et les faire aboutir ailleurs. Ils savent également utiliser – ils ne sont pas bêtes – des algorithmes de chiffrement, tel PGP, nombreux à être considérés comme sécurisés.

En fait, cela reviendra à intercepter de la soupe numérique, illisible ! Les gens qui veulent se cacher sur les réseaux internet savent le faire : ils ne vous ont pas attendu, je vous assure !

Toutes ces questions restent sans réponse. D'autant que votre loi sera publique, ce qui signifie que les utilisateurs ayant des visées terroristes passeront ailleurs – un autre pays, un autre réseau – en plus de le faire de manière chiffrée. Vous les avertissez que vous allez regarder ce qu'ils font. Les gens réellement motivés, qui veulent commettre une infraction et qui savent qu'il y a un gendarme qui utilise telle ou telle technique, auront recours à des moyens détournés. Tout ce que vous intercepterez, c'est de la soupe numérique, comme avec la loi Hadopi, mais les responsables, on ne les coïncera pas.

M. le président. La parole est à M. Pierre Lellouche.

M. Pierre Lellouche. Nous abordons là un domaine qui relève des technologies du futur, extrêmement difficiles à appréhender par le législateur.

Mme Laure de La Raudière. En effet.

M. Pierre Lellouche. Qu'il s'agisse d'interdire une fréquence quand elle est manipulée par des terroristes, qu'il s'agisse de réguler le monde de l'internet, c'est toujours très compliqué parce que la technologie évolue toujours plus vite que la loi.

Plusieurs réflexions me viennent à l'esprit. D'abord, je crois qu'il va falloir évaluer le dispositif dans le temps, voir ce qu'il donne à l'usage. Cet après-midi, nous avons fait tous ensemble un effort pour augmenter le niveau de contrôle. C'est une avancée très importante par rapport à un univers qui suscite énormément d'inquiétudes aussi bien parmi les opérateurs que les internautes.

Ensuite, il faudra se demander si la Commission est efficace en matière de contrôle de ces systèmes d'algorithmes, qui sont très complexes. Je souhaiterais que le Gouvernement nous indique comment, concrètement, la Commission va pouvoir travailler. Aura-t-elle auprès d'elle des experts qui seront en mesure de l'éclairer ?

M. Lionel Tardy. On a déjà posé la question.

M. Pierre Lellouche. C'est bien de prévoir des parlementaires et des juges, mais par définition, nous sommes loin d'être des experts en matière de contrôle de flux cryptés sur le réseau internet. Bref, nous avons augmenté le niveau de contrôle. Assurons-nous donc qu'il fonctionne.

Autre remarque : les États étrangers qui ont mis en place de tels systèmes n'ont pas été épargnés et n'en ont pas moins subi des attentats, notamment les États-Unis.

M. Lionel Tardy. Bien sûr.

M. Pierre Lellouche. L'efficacité des systèmes de surveillance est extraordinairement faible.

Bref, il serait souhaitable de prévoir une sorte de clause de revoyure du dispositif afin d'évaluer l'efficacité du contrôle et de voir s'il sert à quelque chose. Je soupçonne fort, monsieur le ministre de la défense, que ce système complexe et coûteux ne vous aidera en rien.

M. le président. Monsieur Lellouche...

M. Pierre Lellouche. Je conclus, monsieur le président, en répétant que toutes les attaques terroristes que nous avons subies sur notre sol ou qui ont eu lieu dans les pays voisins ont été commises par des gens déjà identifiées.

M. Lionel Tardy. Bien sûr.

M. le président. La parole est à M. Éric Ciotti.

M. Éric Ciotti. Mme Attard a indiqué que le syndicat de police Alliance était opposé à ce texte. Comme j'aime vérifier les informations, je me suis entretenu avec le secrétaire général adjoint de ce syndicat...

M. Pascal Popelin. Par une ligne directe ! (*Sourires.*)

M. Éric Ciotti. ...qui m'autorise d'ailleurs à indiquer la position de cette formation syndicale, la première dans la police nationale. Il a indiqué que le texte allait mieux sécuriser le travail des policiers. Madame Attard, vous vous êtes livrée à quelques démonstrations techniques. Si elles sont aussi pertinentes que vos prises de position politiques, on peut douter de votre argumentation.

M. le président. La parole est à M. Charles de La Verpillière.

M. Charles de La Verpillière. Pour ma part, je ne voterai pas ces amendements identiques. Je comprends que le procédé dont nous parlons est un profilage qui permet, en croisant plusieurs critères, de déceler des comportements suspects. Ce profilage ou ce dispositif me paraît efficace. S'il permet de détecter ne serait-ce qu'une seule menace, son efficacité serait prouvée.

En second lieu, ce procédé me paraît suffisamment entouré de garanties, avec bien sûr l'intervention de la Commission nationale de contrôle, mais surtout, dans ce cas précis, le fait qu'il y ait chronologiquement deux niveaux de décision : d'abord, la décision d'utiliser le dispositif, lequel doit permettre de déceler la menace, ensuite, une nouvelle décision pour procéder à l'identification des auteurs de ces menaces.

Dernier argument : Éric Ciotti et Guillaume Larrivé l'ont très bien démontré, nous sommes face à une menace terroriste gravissime qui s'apparente à notre rencontre à un état de guerre. Dans une guerre, lorsqu'on a un arsenal avec plusieurs catégories d'armes, on ne peut se priver d'aucune d'entre elles. C'est pourquoi je ne voterai pas ces amendements.

M. le président. La parole est à M. Patrick Bloche.

M. Patrick Bloche. Je n'ai qu'une question à poser, qui traduit mon inquiétude, partagée par un certain nombre de parlementaires ici présents ce soir.

Que pourraient devenir les dispositions figurant aux articles 14 à 16, concernant les boîtes noires, dans les mains d'un gouvernement qui ne serait pas aussi républicain, aussi soucieux des libertés publiques et de la protection des données personnelles que celui qui est aux responsabilités en France aujourd'hui ?

M. Christian Paul. Bonne question.

M. le président. La parole est à M. le ministre.

M. Jean-Yves Le Drian, ministre. Sur la question des algorithmes, j'ai exposé l'ensemble des garanties que se proposait d'apporter le Gouvernement, assorties d'éléments complémentaires liés aux discussions que nous avons eues avec les hébergeurs et les opérateurs aujourd'hui, qui feront l'objet d'un amendement.

Monsieur Lellouche, le dispositif sera évalué dans trois ans, y compris la vérification du bon fonctionnement de la CNCTR ainsi que l'évaluation des algorithmes et leur suivi en cours d'exécution.

Monsieur Bloche, j'ai établi tout à l'heure une liste de huit garanties permettant d'éviter toute aventure politique condamnable telle que vous en redoutez.

M. le président. La parole est à M. le rapporteur.

M. Jean-Jacques Urvoas, rapporteur. Monsieur Bloche, la technique existe, nous ne l'inventons pas. Nous essayons de créer une norme pour protéger l'État de droit dans l'utilisation de ces techniques. C'est en renforçant le cadre juridique que nous évitons le dévoiement de techniques qui existent.

(Les amendements identiques n° 25, 146, 185, 228 et 259 ne sont pas adoptés.)

M. le président. Mes chers collègues, vous souhaitez des débats dépassionnés et utiles. Je me suis affranchi du règlement pour permettre à beaucoup d'orateurs de s'exprimer sur cette série d'amendements, au lieu de deux interventions seulement, une pour et une contre. Au regard de l'importance de ce texte et de l'implication de chacun d'entre vous, mon devoir était de faire ainsi mais je ne souhaite pas que chaque amendement suivant fasse l'objet de dix interventions, qui parfois n'ont d'ailleurs rien à voir avec le sujet. Je vous invite à rationaliser vos interventions, sinon j'en reviendrai à l'application stricte du règlement.

La parole est à Mme Laure de La Raudière, pour soutenir l'amendement n° 104.

Mme Laure de La Raudière. Le présent amendement est de même nature que les précédents et concerne la suppression du dispositif des « boîtes noires ». Nous avons encore quelques questions à vous poser, monsieur le ministre. Vous avez cité les algorithmes de profilage qui existent chez les géants d'internet. J'espère que ce ne sont pas des algorithmes de cette nature que vous avez utilisés, car nous sommes tous conscients qu'ils ne sont pas très efficaces : on vous propose des amis qui ne correspondent pas forcément à votre profil ! On vous en propose beaucoup, donc il y a forcément des erreurs !

Les algorithmes disponibles en matière de profilage ne sont pas suffisamment performants par rapport à la matière que vous visez, c'est-à-dire la lutte contre le terrorisme. Il ne s'agit pas d'acheter des chaussures ou des vêtements ! La comparaison que vous avez établie tout à l'heure ne me semble donc pas très appropriée.

Il serait donc utile que vous nous précisiez quel type d'algorithme vous allez utiliser pour avoir des algorithmes plus performants que ceux que peuvent acheter les géants d'internet. En effet, si ces derniers pouvaient mieux cibler les offres qu'ils proposent, ils n'hésiteraient pas à le faire ! Et, comme vous le savez, ce sont les entreprises capitalistiques les plus puissantes au monde qui sont capables de se payer les meilleurs ingénieurs d'analyse de bases de données...

L'efficacité des algorithmes est une vraie question. Nous avons des inquiétudes à cet égard par rapport à l'atteinte aux libertés individuelles. Si ces algorithmes ne sont pas efficaces, cela ne vaut pas la peine d'en parler dans la loi et de susciter autant de questions dans le public.

M. Pierre Lellouche. Très bien.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé cet amendement. Mme de La Raudière a expliqué qu'elle était contre l'algorithme. Je n'ai pas d'autre argument que celui de dire que nous sommes opposés au principe de cet amendement dans la mesure où l'Assemblée nationale vient de refuser de supprimer l'algorithme.

(L'amendement n° 104, repoussé par le Gouvernement, n'est pas adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 26.

M. Lionel Tardy. Amendement de repli. Étant donné le caractère potentiellement intrusif des boîtes noires, il faut sortir l'artillerie lourde et passer par un avis conforme de la

CNCTR pour l'identification des personnes. Cela voudrait dire que le Premier ministre ne pourrait passer outre un avis négatif.

S'il y a bien un dispositif pour lequel cet avis conforme est nécessaire, c'est celui-ci. Ce serait de nature à rassurer un minimum. Tel est le sens de mon amendement.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé cet amendement. Nous avons passé une heure sur ce sujet lundi, et une heure mardi. Cela n'est peut-être pas la peine de repasser une heure pour dire que nous sommes contre le fait que l'autorité administrative ait le pouvoir de décision. C'est la prérogative de l'exécutif.

(L'amendement n° 26, repoussé par le Gouvernement, n'est pas adopté.)

M. le président. La parole est à M. le ministre, pour soutenir l'amendement n° 382.

M. Jean-Yves Le Drian, ministre. Le présent amendement a pour objet de dissiper les inquiétudes qui pourraient encore subsister s'agissant de ce dispositif après toutes les explications que nous avons apportées il y a un instant, le ministre de l'intérieur et moi-même.

Comme dans le droit commun de l'usage des techniques de renseignement, l'autorisation du Premier ministre est accordée pour quatre mois. Le dispositif ne pourra être réutilisé qu'après réexamen et appréciation de son utilité.

De façon plus générale, le Gouvernement déposera en fin de texte un amendement tendant à donner une durée déterminée, jusqu'à fin 2018, au dispositif de la détection par algorithme. Cela permettra de s'assurer qu'il s'agit d'un dispositif utile qui ne porte pas une atteinte disproportionnée aux libertés publiques ainsi qu'on a pu l'entendre dans quelques interventions et publications. Je confirme ainsi ce que j'ai indiqué tout à l'heure dans mon propos liminaire concernant les algorithmes.

(L'amendement n° 382, accepté par la commission, est adopté.)

M. le président. Je suis saisi d'un amendement n° 437 qui fait l'objet de plusieurs sous-amendements, nos 443, 441 et 442.

La parole est à M. le ministre de l'intérieur, pour soutenir l'amendement.

M. Bernard Cazeneuve, ministre de l'intérieur. Comme je l'ai déjà indiqué, nous avons reçu, avec M. Emmanuel Macron et Mme Axelle Lemaire, les représentants des principaux hébergeurs français de sites internet, qui nous ont fait part de leurs inquiétudes sur certains aspects du projet de loi sur le renseignement. Le Gouvernement, vous le savez, est particulièrement attaché à soutenir la compétitivité d'un secteur en croissance, qui crée des emplois dans notre pays. Rien dans ce projet n'entrave le développement de ces entreprises stratégiques et nous ne souhaitons en aucun cas dégrader la très forte confiance dont leurs clients les créditent.

Les hébergeurs, auxquels nous avons expliqué quels étaient l'esprit de cette loi et les dispositions que nous prenions précisément pour encadrer l'activité des services de renseignement et leurs techniques – car tel est bien l'objectif premier de ce projet de loi –, ont précisé quelles étaient

leurs inquiétudes, au terme de quoi nous avons souhaité proposer un amendement qui permette de conforter encore les garanties offertes par ce texte pour assurer le contrôle de l'activité des services de renseignement.

Cet amendement apporte donc une garantie supplémentaire – nous en avons déjà donné beaucoup et en donnerons encore autant qu'il sera nécessaire pour rassurer chacun sur le fait qu'il n'y a pas de surveillance de masse, mais seulement des dispositifs très ciblés, qui ne s'appliquent du reste qu'à la lutte contre le terrorisme.

L'amendement précise essentiellement trois points. En premier lieu, la technique sera soumise au principe de proportionnalité et de nécessité qui figure déjà dans la loi. La surveillance sur données anonymes s'effectuera sur les seuls traitements de données strictement nécessaires à la détection de la menace terroriste. Cela figure déjà dans le texte, mais l'amendement le précise, le conforte et le répète.

En deuxième lieu, les opérateurs qui le souhaitent pourront eux-mêmes, comme ils l'ont demandé, séparer les métadonnées des contenus, afin de pouvoir garantir eux-mêmes que les contenus ne feront pas l'objet de ce mode de détection. Les procédures d'urgence ne seront pas applicables à cette technique de renseignement.

Ces garanties s'ajoutent à celles déjà énoncées par le texte. L'utilisation du dispositif sera, je le répète, strictement limitée à la finalité de la prévention du terrorisme, ainsi que le prévoyait explicitement, dès l'origine, le projet initial du Gouvernement.

Par ailleurs, d'autres amendements du Gouvernement prévoient que le dispositif fera l'objet d'une expérimentation jusqu'en 2018, délai à l'issue duquel il appartiendra au Parlement, sur la base d'une évaluation concrète de ce dispositif, de le maintenir ou non, ainsi que l'a annoncé lundi le Premier ministre.

L'autorisation d'utiliser un algorithme aura une validité de quatre mois renouvelables, ce qui fournira à la CNCTR l'occasion de se prononcer régulièrement sur la proportionnalité du dispositif à sa finalité antiterroriste.

En troisième lieu, la CNCTR pourra être saisie par l'ARCEP, notamment s'il existe des interrogations quant à l'effet du dispositif sur le fonctionnement des réseaux. Par ailleurs, les dispositifs seront mis en œuvre en concertation avec l'ensemble des opérateurs – j'insiste sur ce point –, comme c'est déjà le cas dans le cadre judiciaire ou, par exemple, pour les interceptions de sécurité.

Comme l'a déjà indiqué tout à l'heure M. Le Drian, ce texte a pour objectifs de mieux protéger les Français, de sécuriser sur le plan juridique les pratiques des services de renseignements et d'exercer sur eux, dans le cadre de la mobilisation des techniques, un contrôle très puissant, à la fois administratif, juridictionnel et parlementaire. Cet amendement est de nature à conforter encore la puissance du dispositif de contrôle que nous mettons en place.

M. le président. La parole est à M. Sergio Coronado, pour soutenir le sous-amendement n° 443.

Monsieur Coronado, vous pouvez défendre également votre sous-amendement n° 442.

M. Sergio Coronado. Je commencerai par mon sous-amendement n° 442.

L'article L. 861-3 est issu de l'article L. 242-9 du code de la sécurité intérieure, qui indique : « Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications ne peuvent être effectuées que sur ordre du ministre chargé des communications électroniques ou sur ordre de la personne spécialement déléguée par lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs dans leurs installations respectives. »

Il n'évoque que la mise en place des traitements, alors que dans l'exposé sommaire de son amendement le Gouvernement indique que « Les opérateurs auront la possibilité, ainsi que le précise le renvoi à l'article L. 861-3 du code de la sécurité intérieure, de s'assurer par eux-mêmes que les données de contenu seront exclues de la mise en œuvre de ces traitements. » Il s'agit donc d'harmoniser l'amendement avec son exposé sommaire.

M. le président. La parole est à M. Lionel Tardy, pour soutenir le sous-amendement n° 441.

M. Lionel Tardy. Monsieur le président, j'aurais souhaité m'exprimer également sur l'amendement du Gouvernement.

M. le président. Je vous propose de présenter votre sous-amendement. Vous pourrez également évoquer l'amendement du Gouvernement.

M. Lionel Tardy. Essayons de trouver des solutions maintenant, sans quoi vous serez obligés de réunir à nouveau les hébergeurs à Bercy. Il s'agit de prévoir que seules des métadonnées seront recueillies, et surtout pas des données de contenu ou de navigation. Ce sous-amendement vise à fixer explicitement le périmètre des métadonnées – connexion, localisation, identification du terminal – en renvoyant, en plus de ce qui est prévu, à l'article L. 34-1 du code des postes et télécommunications électroniques. Je précise que je fais référence au VI de cet article, ce qui n'est pas précisé dans l'amendement, car il s'agit d'une procédure administrative et le droit de communication se fonde sur le renvoi explicite à l'article.

Ce renvoi est utile, car l'article en question précise que ces données « ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications » et que « Les opérateurs prennent toutes mesures pour empêcher l'utilisation de ces données à des fins autres que celles prévues au présent article. » C'est là exactement ce que vous voulez et ce qu'il faut. Seule l'adoption de ces sous-amendements et de l'ensemble de ces critères cumulatifs permettra d'assurer que les données de contenu sont exclues.

M. le président. Le sous-amendement n° 442 a déjà été défendu.

Quel est l'avis de la commission sur l'amendement du Gouvernement et sur ces trois sous-amendements ?

M. Jean-Jacques Urvoas, rapporteur. La commission n'a, bien entendu, pas pu étudier l'amendement du Gouvernement, qui a été déposé dans la journée – on en comprend bien les raisons, car il procède d'une réunion qui s'est tenue aujourd'hui entre le Gouvernement et les hébergeurs, de telle sorte qu'il était donc matériellement impossible que la commission puisse l'analyser.

Compte tenu de l'argumentation de M. le ministre, le rapporteur émet un avis favorable, car cet amendement n'a pour but que de préciser que le Premier ministre garantira un champ technique particulier, que les opérateurs auront la possibilité de s'assurer eux-mêmes que les données de contenu seront exclues et que la procédure d'urgence ne s'appliquera pas. Je ne vois donc pas pourquoi nous nous opposerions à cet amendement.

J'émetts en revanche un avis très défavorable sur le sous-amendement n° 442, car il ne faut pas transformer les rôles en matière de contrôle. Dans ce projet de loi, en effet, le contrôle relève de la CNCTR : demander que ce soient les opérateurs et les personnes qui puissent contrôler la mise en œuvre des traitements est donc contraire à l'esprit du texte.

Quant aux deux autres sous-amendements, n°s 443 et 441, qui ont le même objet, leur plus-value ne semble pas évidente. Avis défavorable, donc.

M. le président. Quel est l'avis du Gouvernement sur les trois sous-amendements ? Qui, de M. le ministre de l'intérieur ou de Mme la garde des sceaux, donne cet avis ?

M. Bernard Cazeneuve, ministre de l'intérieur. Avis défavorable.

M. le président. La parole est à M. Lionel Tardy.

M. Lionel Tardy. L'amendement n° 437 du Gouvernement est surréaliste. En commission, vous avez été alertés sur les problèmes posés par les boîtes noires, que je viens de rappeler.

M. Jean-Yves Le Drian, ministre. Il n'y a pas de boîtes noires !

M. Lionel Tardy. Puis, il a fallu une pétition sur Internet et que les hébergeurs menacent de se délocaliser pour qu'ils soient reçus en urgence, aujourd'hui, à Bercy et que vous acceptiez de faire un geste. Monsieur le ministre, je salue ce geste, mais je doute très sincèrement de sa réalité et je vais maintenant m'efforcer de décrypter votre amendement.

Sur ce que vous présentez comme trois évolutions, une seule est réelle : le fait que la procédure d'urgence absolue – qui ne requiert pas d'avis préalable de la CNCTR – ne soit pas applicable au dispositif, non plus que l'urgence opérationnelle, dont nous parlerons très prochainement.

Pour les deux autres, vous dites que l'autorisation du Premier ministre respectera le principe de proportionnalité et précisera le champ technique. Cela ne veut pas dire grand-chose et, en outre, ce ne sont là que des mots.

Monsieur le rapporteur, alors que vous avez dit à l'article 1^{er} que la proportionnalité coulait de source, vous la mentionnez de nouveau ici. Par ailleurs, les boîtes noires étaient déjà limitées à la lutte contre le terrorisme : rien de neuf, donc, à ce propos.

Je passe sur la deuxième phrase, qui figurait déjà dans le texte initial. Vous dites ensuite que les opérateurs pourront s'assurer eux-mêmes de la proportionnalité. Pardonnez ma franchise, mais c'est totalement faux : le futur article L. 861-3 ne dit absolument pas cela, mais que l'installation devra être faite par des agents, sur autorisation du Premier ministre. Prétendre autre chose serait mentir. Là non plus, donc, rien de neuf.

Je suis donc désolé, mais, hormis la suppression de l'urgence – que je salue, mais qui n'est qu'un pas mineur –, tous les problèmes demeurent. Ces dispositions restent des obligations franco-françaises. La meilleure garantie aurait été un avis conforme de la CNCTR, comme je viens de le proposer.

Cet amendement ne peut donc raisonnablement rassurer personne – ni les hébergeurs, ni moi – sur le dispositif. J'y suis donc opposé.

M. le président. La parole est à Mme Isabelle Attard.

Mme Isabelle Attard. Avec cet amendement n° 437 du Gouvernement, qui vient d'arriver, c'est presque pire qu'avant, car vous demandez, en somme, que les hébergeurs eux-mêmes installent ce dispositif, devenant donc – vous pouvez m'interrompre si je m'abuse – des auxiliaires du renseignement, tout en n'ayant toujours aucune maîtrise de l'algorithme. L'argument selon lequel il n'y a pas de violation de la vie privée, utilisé également par la NSA, est faux.

Je souhaiterais ensuite que vous répondiez à une question très précise : en instaurant ce mécanisme de boîtes noires et d'algorithmes, comment vous assurez-vous que, dans un futur très proche, ces boîtes noires ne seront pas piratées ? Je crains en effet que ce piratage ait lieu.

C'est très bien de vous poser en protecteur de notre vie privée et des libertés individuelles, comme vous l'avez fait, avec d'autres ministres, depuis plusieurs jours, mais s'il y a un piratage – peut-être devrais-je dire plutôt : « lorsqu'il y aura un piratage » –, ces données, qui ne devraient être utilisées que par des gens bienveillants de la CNCTR ou de nos services de renseignement, qui savent faire leur travail, tomberont un jour entre les mains de personnes qui, elles, ne seront nullement bienveillantes. Peut-être avez-vous déjà fait travailler vos services sur cette question. Comment éviterez-vous le futur piratage de ces boîtes noires ?

(Les sous-amendements n°s 443, 441 et 442, successivement mis aux voix, ne sont pas adoptés.)

(L'amendement n° 437 est adopté.)

M. le président. La parole est à M. Jean-Jacques Candelier, pour soutenir l'amendement n° 147.

M. Jean-Jacques Candelier. Il s'agit d'un amendement de repli, qui fait suite à notre amendement n° 146 de suppression du nouvel article L. 851-4. Le dispositif prévu par cet article porte en effet atteinte aux libertés individuelles de nombreuses personnes, indistinctement et simultanément. Or, comme le souligne très justement l'Union syndicale des magistrats, dès lors que de telles mesures sont vouées à assurer la surveillance de personnes soupçonnées de terrorisme, l'ouverture d'une enquête judiciaire apparaît nécessaire. Tel est en particulier le cas lorsqu'une menace de terrorisme est révélée. Au risque de m'attirer les foudres ministérielles, j'irai jusqu'au bout : nous proposons donc d'ajouter au dispositif légal l'instauration d'un contrôle par l'autorité judiciaire.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Sans surprise, la commission a émis un avis défavorable à cet amendement car, depuis le début, nous expliquons que nous nous situons dans le domaine de la police administrative et qu'il convient donc d'éviter les confusions avec la police judiciaire.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre de la défense. Même avis. *(L'amendement n° 147 n'est pas adopté.)*

M. le président. La parole est à M. Denys Robiliard, pour soutenir l'amendement n° 284.

M. Denys Robiliard. Si vous le permettez, monsieur le président, je défendrai en même temps l'amendement n° 285, car les deux sont liés.

Je commencerai par une explication – mais vous pouvez également me démentir, monsieur le ministre, si je n'ai pas bien compris le système – : à la lecture des trois alinéas de l'article L. 851-4, dont nous débattons, je comprends, par analogie avec le fonctionnement de l'usine de traitement des eaux de ma ville, qu'il y a un filtre. À Blois, l'eau de la Loire passe d'abord dans un filtre contenant des bactéries puis, en cas de pollution anormale, une luminescence apparaît et l'usine s'arrête. Je ne développe pas la suite du traitement parce que ce serait faire de la publicité pour le vin !

L'algorithme, qui opère un traitement minimal sur un ensemble de communications, agit comme un filtre. Les personnes ne sont pas identifiées ; seuls les éléments permettant de repérer un potentiel terroriste sont détectés. Le traitement massif des données imposé aux opérateurs ne permet toutefois pas aux services de renseignement d'accéder au système. J'aimerais que cela soit confirmé : avons-nous bien compris ou non ?

Ce n'est que dans un deuxième temps, si une menace est révélée, que le Premier ministre demande l'avis de la Commission nationale de contrôle des techniques de renseignement. Dans un premier temps, le filtre est général ; puis, en cas d'alerte, on va chercher les données. C'est comme cela du moins que je comprends les premier et deuxième alinéas.

J'avoue que je m'interroge sur le moment auquel on sollicite l'avis de la Commission nationale de contrôle. J'ai l'impression que cet avis n'est plus préalable puisque, lorsque le Premier ministre – ou l'une des personnes déléguées par lui – décide d'avoir recours à la technique, il peut, après avis de cette commission, l'imposer aux opérateurs et la mettre en application. Ce n'est que quand la Commission en a le temps, si je comprends bien, qu'elle donne son avis et émet des recommandations. Est-ce préalable ou non ?

Je souhaite juste un éclaircissement sur le fonctionnement de ce système relativement complexe, y compris dans la façon dont il est présenté dans cet article. En fonction de votre réponse, je vous indiquerai si je maintiens ou non mon amendement.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Les deux amendements n°s 284 et 285 portaient, au-delà des questions posées par Denys Robiliard, sur l'avis conforme. Sur ce point, l'avis de la commission est défavorable. Quant au moment où l'avis intervient, du point de vue de la commission, l'avis étant préalable, il intervient avant que le dispositif ne soit imposé.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Le rapporteur ayant apporté les explications, je serai bref : le contrôle et la référence à la CNCTR ont lieu avant, pendant et après. On ne peut pas être plus clair ! Si un algorithme change entre-temps, il est de nouveau soumis à la CNCTR pour avis avant d'être mis en œuvre et avant que le Premier ministre ne prenne une décision. J'ai déjà donné toutes les explications nécessaires à ce sujet tout à l'heure.

J'ajoute que, dans les propos tenus par les uns et par les autres, une expression revient sans cesse : celle de « boîte noire ». Or il n'y a pas de « boîte noire » ! Il y a la plus grande transparence par les hébergeurs et par les opérateurs dans la mise en œuvre des dispositifs que nous avons votés il y a un instant.

M. Lionel Tardy. On sait ce qu'il y a dans la boîte noire !

M. le président. La parole est à M. Denys Robiliard.

M. Denys Robiliard. Je me suis expliqué hier longuement : je ne vais donc pas revenir sur ce sujet, n'ayant pas l'intention que l'on y passe une heure. Un avis conforme – demander sa conformité a du sens puisque cet avis est préalable – me paraissait utile et protecteur. Le système que j'ai décrit ne me paraît pas démenti par ce que vous avez dit. En outre, je n'ai jamais parlé de « boîte noire » ! J'ai simplement parlé d'un filtre.

M. Jean-Yves Le Drian, ministre. Je ne disais pas cela pour vous !

M. Denys Robiliard. Je maintiens qu'en termes de garantie pour chacune des personnes susceptibles d'utiliser internet, le système de l'avis conforme me paraît meilleur, davantage protecteur des libertés ; j'ajoute que si l'avis est préalable et qu'il doit être conforme, je suis certain que les moyens nécessaires seront, dans le temps, mis à la disposition de la CNCTR. Je crains sinon qu'on ne lui donne pas tous les moyens nécessaires à ces contrôles.

M. Lionel Tardy. Tout à fait !

(L'amendement n° 284 n'est pas adopté.)

M. le président. Monsieur Robiliard, vous avez déjà défendu l'amendement n° 285. Le retirez-vous ?

M. Denys Robiliard. Il est retiré.

(L'amendement n° 285 est retiré.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 27.

M. Lionel Tardy. Le présent amendement vise à apporter une solution à un problème très épineux mais très intéressant, soulevé par Jean-Marie Delarue. Il propose en substance que la CNCTR ait également accès au dispositif une fois celui-ci en marche. La CNCTR pourra en principe en observer et en contrôler le fonctionnement. Mais elle est dépendante des informations fournies par les services et du mécanisme tel qu'il fonctionne. Elle n'a donc pas de vue sur le dispositif, sur la « boîte noire » en elle-même : son contrôle n'est donc que partiel. Cette faille a été corrigée en partie en commission des lois, ce que je salue : la CNCTR aura un accès permanent au dispositif et pourra émettre un avis sur lui ainsi que sur les critères des fichiers.

C'est un premier pas, mais un aspect a été oublié : si le dispositif est modifié en cours de route, la CNCTR a certes un accès permanent, mais elle ne peut plus émettre d'avis. L'amendement n° 27 propose donc que la procédure d'avis vaille lors de la création mais aussi lors de chaque modification du dispositif et des critères du traitement automatisé visant à détecter les potentiels terroristes.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Je ne comprends absolument pas l'amendement déposé par notre collègue Tardy et je crains que son explication ne vienne encore embrouiller son propre texte. Selon la deuxième phrase de l'alinéa 16, la Commission « dispose d'un accès permanent à ceux-ci, est informée de toute modification apportée et peut émettre des recommandations. » Je ne vois pas ce que vous proposez de plus : je crains que vous n'ayez lu le texte que dans sa version antérieure à la modification apportée par la commission des lois. L'avis est défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Même avis.

(L'amendement n° 27 n'est pas adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 413.

M. Lionel Tardy. Il s'agit d'un nouveau point noir concernant le recueil d'informations par les dispositifs spéciaux. On a beaucoup parlé des IMSI-catchers, ces fausses antennes servant à capter des données liées aux terminaux ; mais, en fait, cette partie concerne tous les dispositifs permettant l'enregistrement, la captation. C'est très subtil car l'IMSI-catcher en 3G ou 4G ne peut pas recueillir grand-chose, excepté les références des terminaux.

En fait, c'est même beaucoup plus large que cela : sauf erreur de ma part, l'article 226-3 du code pénal auquel il est fait référence renvoie à différents dispositifs permettant des interceptions de correspondance, des captations de conversation et des enregistrements de données informatiques. Vous voyez que tout cela ne concerne pas que les terminaux et les IMSI-catchers ; c'est l'un des rares points sur lesquels le texte initial était plus protecteur. Je n'ai pas compris les raisons de cette extension, étant donné le caractère intrusif des dispositifs en question.

Cet amendement propose donc de revenir au texte initial en prévoyant que seules peuvent être recueillies les données techniques de connexion strictement nécessaires à l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données techniques relatives à la localisation des équipements terminaux utilisés. De fait, cette limitation des données est salutaire car elle limite également la liste des dispositifs pouvant être utilisés par le biais de cet article précis.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable car la commission a longuement discuté de cet outil – nous avons d'ailleurs un désaccord sur cet aspect avec le Gouvernement, lequel a l'intention d'évoquer à nouveau ce point tout à l'heure.

Nous avons en effet considéré que l'article visant à créer ces dispositions n'avait pas lieu d'être, justement parce que la loi risquait d'être frappée assez rapidement de caducité du fait de

l'évolution technologique. Il nous a paru plus intéressant de traiter ces dispositifs au regard des finalités qu'ils développent. Nous les avons donc réintégrés dans les articles à chaque fois que la finalité était concernée.

Pour ce qui est des interceptions de sécurité, qu'elles soient effectuées au moyen d'un IMSI-catcher ou de tout autre outil, ce qui nous intéresse, ce sont les interceptions de sécurité. Il en va de même pour ce qui est de la collecte des données de connexion : peu importe l'outil, c'est la finalité qui compte. De même, pour l'accès au contenu, peu importe l'outil, c'est la finalité qui compte.

C'est la raison pour laquelle nous avons supprimé le dispositif : nous l'avons réintroduit à chaque fois que nécessaire, parce que nous légiférons en fonction des finalités et non pas des avancées technologiques. Avis défavorable sur votre amendement.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. M. Tardy propose en fait de rétablir la version initiale du texte du Gouvernement. Mais le Gouvernement est soucieux de coproduire ce texte avec le Parlement ; or un dispositif a été trouvé en commission, auquel le Gouvernement a décidé de se rallier.

(L'amendement n° 413 n'est pas adopté.)

M. le président. Je suis saisi de deux amendements, n°s 186 et 28, pouvant être soumis à une discussion commune.

La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 186.

M. Sergio Coronado. Nous allons nous intéresser au texte issu des travaux de la commission. Dans l'esprit rappelé à l'instant par le rapporteur, il s'agit de circonscrire l'autorisation de certaines techniques de recueil de renseignement, en tout cas les plus intrusives, à certaines finalités. Sur le modèle de ce qui a été fait en commission, le présent amendement propose que les techniques de recueil de renseignement les plus intrusives répondent à des finalités parfaitement circonscrites.

Elles sont les suivantes : l'indépendance nationale ; l'intégrité du territoire et la défense nationale ; la prévention du terrorisme ; la prévention de la criminalité et de la délinquance organisées et la prévention de la prolifération des armes de destruction massive.

Les techniques concernées seraient le recours à l'IMSI-catcher et aux dispositifs techniques de proximité, la géolocalisation et l'interception des correspondances électroniques. Ces techniques de renseignement sont fortement intrusives : même le ministre l'a reconnu. Il est donc légitime qu'elles ne soient utilisées que pour des finalités bien précises que j'ai indiquées.

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 28.

M. Lionel Tardy. Avec ces dispositifs, nous avons affaire à des outils très intrusifs, d'autant qu'il sera très difficile de ne pas embarquer en même temps les données de personnes qui ne sont soupçonnées de rien du tout.

Pour les autres dispositifs intrusifs, à savoir les boîtes noires et le recueil en temps réel, vous aviez pris le soin de préciser que seule la lutte contre le terrorisme était concernée. Il faut en faire de même ici : ce sera un moindre mal et si, comme

vous le prétendez, ce ciblage des motifs est réellement efficace, les risques d'intrusion seront limités – davantage qu'avec ce que vous proposez ici. Le sens de mon amendement est donc de les limiter à la lutte contre le terrorisme.

M. le président. Quel est l'avis de la commission sur ces deux amendements en discussion commune ?

M. Jean-Jacques Urvoas, rapporteur. Nous avons une divergence absolue avec les deux amendements qui viennent d'être défendus : nous proposons d'encadrer globalement les dispositifs au regard des finalités. Dès lors que nous avons un cadre strict, extrêmement protecteur – à l'inverse de ce qui avait pu être écrit auparavant ; nous avons longuement débattu sur ce point –, il n'y a aucune raison d'en restreindre les finalités. Il faut permettre à nos services une flexibilité dans l'usage puisque le contrôle est garanti.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(Les amendements n°s 186 et 28, successivement mis aux voix, ne sont pas adoptés.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 29.

M. Lionel Tardy. Concernant le recueil sur le réseau, je ne voyais pas de quel document on pouvait parler ; mais là, je le vois encore moins ! Vous persistez à nous parler de « documents » : c'est très étrange !

Si on lit bien, les dispositifs techniques mentionnés au 1° de l'article 226-3 du code pénal ne concernent que le fait d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par voie électronique ; le fait de capter, d'enregistrer ou de transmettre, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; fait d'accéder en tout lieu à des données informatiques, de les enregistrer, de les conserver et de les transmettre telles qu'elles s'affichent sur un écran.

Là encore, où sont les documents ? Je ne vois que des données. Je répète en outre, car cela est passé relativement inaperçu, que les IMSI-catchers ne sont pas seuls concernés : la liste est beaucoup plus large. En principe, seules les données de connexion sont concernées. C'est ce que prévoyait le texte initial, mais on s'y perd.

Toute l'inquiétude vient du fait que la liste des données n'est pas fixée exhaustivement, ainsi que je l'ai dit tout à l'heure. Il faut donc encadrer ce recueil au maximum et éliminer ce qui peut l'être, à savoir les documents.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. M. Tardy nous a proposé quatre fois le même amendement, nous l'avons repoussé quatre fois et nous allons le repousser une cinquième fois puisque nous considérons que le décret du 24 décembre 2014, pris en application de la loi de programmation militaire, a levé toutes les éventuelles craintes qui avaient pu alors être formulées.

M. Lionel Tardy. Nous n'avons toujours pas de réponse !

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 29 n'est pas adopté.)

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 187.

M. Sergio Coronado. Cet amendement propose que les IMSI-catchers fassent l'objet d'une homologation préalable de la CNCTR avant d'être utilisés par les services. Vous le savez, une grande diversité de dispositifs existe, certains pouvant être particulièrement intrusifs, voire attentatoires à la vie privée des citoyens.

L'objet du présent amendement est double : d'abord, s'assurer que les dispositifs utilisés ne seront pas plus attentatoires au secret des correspondances que nécessaire et, ensuite, s'assurer que des fonctions de traçabilité seront bien déployées sur ces dispositifs pour assurer un suivi des données captées.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Malheureusement, la commission a donné un avis défavorable, puisque la précision paraît inutile : une commission existe, celle qui est prévue à l'article L. 226-2 du code pénal, laquelle est compétente pour l'ensemble des questions de ce type. Il n'y a donc pas besoin d'en créer une nouvelle.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 187 n'est pas adopté.)

M. le président. Je suis saisi de trois amendements, n° 357, 30 et 188, pouvant être soumis à une discussion commune.

Les amendements n° 30 et 188 sont identiques.

La parole est à M. Pascal Popelin, pour soutenir l'amendement n° 357.

M. Pascal Popelin. Nous n'étions pas allés au bout de la discussion sur les questions de délai lors de l'examen du texte en commission. C'est pourquoi nous avons adopté hier soir, à partir d'une suggestion du groupe SRC que j'ai eu l'honneur de présenter, un amendement portant sur les délais de conservation des renseignements collectés dans le cadre des dispositifs visés à l'article 1^{er}.

Le présent amendement a pour objet d'harmoniser les délais permettant aux services de renseignement de discriminer les données collectées au moyen d'un dispositif de sécurité, en passant de 30 à 90 jours.

Je précise que le délai prévu compte parmi les plus faibles d'Europe : en Allemagne, pays où tout cela existe déjà, la législation fixe ce délai à six mois.

Je veux aussi indiquer que le recoupement des données recueillies, puisque dans le cadre en question les services ne sont autorisés à collecter que des données techniques de connexion et n'ont pas accès aux contenus, ce recoupement, disais-je, prend beaucoup de temps.

En outre, dans le cadre de filatures complexes d'individus formés aux techniques de contre-filature, il est impossible d'effectuer un recoupement rapide sans exposer les agents ou révéler la surveillance.

Enfin, je rappelle que le recours à ces techniques est strictement encadré, le président Urvoas vient de le rappeler, pour garantir la probité de leur usage. Nous proposerons encore de renforcer cet encadrement dans un amendement qui va être appelé juste après ceux-ci.

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 30.

M. Lionel Tardy. Vous n'en serez pas étonnés, je pense l'inverse : le gros risque serait que des interceptions concernent des personnes qui n'ont rien à voir avec les finalités du renseignement. Or le texte précise que les informations recueillies seront détruites dès qu'il apparaît qu'elles ne sont pas en rapport avec l'autorisation de mise en œuvre, dans un délai de 30 jours.

Je regrette : pour moi, 30 jours, c'est trop long. C'est la même durée de conservation que pour les interceptions de sécurité qui, elles, concernent des personnes ciblées. Il faut donc réduire cette durée de conservation et que la destruction soit la plus rapide possible. Mon amendement vise donc à ramener le délai de 30 à 10 jours de délai.

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 188.

M. Sergio Coronado. Nous avons déjà eu ce débat en commission, et l'avons encore eu hier. Nous sommes opposés à l'allongement des délais. Comme notre collègue Tardy, nous trouvons qu'une durée de conservation de 30 jours est extrêmement longue et nous souhaitons la réduire à 10. Mais j'imagine qu'après l'allongement des délais voté hier, l'Assemblée fera de même ce soir.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a été plus sensible aux arguments de Pascal Popelin qu'à ceux de Lionel Tardy ou de Sergio Coronado. Nous avons donc donné un avis favorable à l'amendement n° 357.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 357 est adopté. En conséquence, les amendements n° 30 et 188 tombent.)

M. le président. Je suis saisi de deux amendements identiques, n° 358 et 395.

La parole est à M. Pascal Popelin, pour soutenir l'amendement n° 358.

M. Pascal Popelin. Autant il faut que les techniques de renseignement puissent être utilisées de manière efficace, autant il faut que leur usage soit parfaitement encadré. Pour renforcer cet encadrement, mon amendement prévoit que les dispositifs de proximité, en plus d'être inscrits dans un registre spécial contrôlé par la CNCTR, fassent l'objet d'un contingentement limitant leur utilisation simultanée, à l'image de ce qui se pratique en matière d'interceptions de sécurité.

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 395.

M. Sergio Coronado. Je me félicite que le travail du groupe écologiste inspire parfois le groupe SRC. Je ne referai pas la défense qui a été brillamment faite et j'imagine que,

M. Popelin ayant un plus grand pouvoir de conviction que nous, comme l'a rappelé notre rapporteur, les deux amendements recevront un avis favorable.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Je ne sais pas qui a inspiré qui, mais comme le montrent les numéros d'ordre, l'amendement du groupe SRC est arrivé avant celui du groupe écologiste. Mais en l'espèce, l'intelligence est mutuelle et les profits partagés, puisque la commission a donné un avis favorable aux deux amendements.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(Les amendements identiques n° 358 et 395 sont adoptés.)

M. le président. Je suis saisi d'un amendement n° 380 deuxième rectification qui fait l'objet d'un sous-amendement n° 412.

La parole est à M. le ministre, pour soutenir l'amendement.

M. Bernard Cazeneuve, ministre. Nous avons eu plusieurs discussions sur ce sujet. Pour dire les choses simplement, cet amendement vise à rétablir l'urgence opérationnelle.

Vous vous souvenez qu'il y a eu une discussion sur ce sujet avec le rapporteur, qui proposait de ne prévoir qu'un seul dispositif d'urgence en fusionnant l'urgence absolue et l'urgence opérationnelle. Hier soir, j'ai eu l'occasion de dire les raisons pour lesquelles il fallait distinguer l'une de l'autre et pourquoi nous avons besoin d'un dispositif particulier à l'urgence opérationnelle. Par conséquent cet amendement, dans la continuité des discussions que nous avons eues hier, tend à rétablir ce régime.

M. le président. La parole est à M. Lionel Tardy, pour soutenir le sous-amendement n° 412.

M. Lionel Tardy. Voici donc le second régime d'urgence, le pire à mes yeux : l'urgence opérationnelle. C'est étrange, mais une urgence est plus urgente que l'autre !

Je dis que c'est le pire des deux régimes, parce qu'on zappe non seulement l'avis de la CNCTR, mais aussi l'autorisation du Premier ministre. Si j'ai bien compris, les agents décident seuls : toute l'architecture de la procédure est bouleversée.

C'est en cas de menace imminente, pour prévenir les risques, mais des garanties sont possibles. Voici ce que disait M. Delarue à l'agence de presse AEF sur ce régime d'urgence, un point de vue que je partage totalement...

M. Pascal Popelin. M. Tardy n'est pas capable de penser par lui-même !

M. Lionel Tardy. Il y a des spécialistes ! Moi, je ne lis pas *L'Obs*, j'écoute les spécialistes. Et M. Delarue n'est pas n'importe qui.

Voici ce qu'il déclarait : « Certes, la technique devra être régularisée sous quarante-huit heures, mais en matière d'enquête, c'est beaucoup. Il se pourrait très bien qu'un service place une balise, la retire avant quarante-huit heures et ne demande même pas la régularisation. Je suis favorable au fait de donner une grande latitude de travail aux services de renseignement, mais si un service peut procéder à des actes d'enquête tout seul, sans en référer à qui que ce soit pendant

un certain délai, nous ne sommes plus dans l'équilibre souhaitable. Le texte donne la possibilité aux services de faire pendant un temps déterminé ce que bon leur semble, y compris à l'insu de leur propre ministre. Alors, même si vous proposez de passer de quarante-huit à vingt-quatre heures, c'est bien mais le problème reste et ce n'est pas pour rien que le rapporteur avait supprimé cette urgence en commission. »

A minima, pour répondre aux interrogations de M. Delarue, je propose encore une fois d'ajouter que les transcriptions des données collectées en application du présent article sont transmises à la CNCTR, qui veille au caractère nécessaire et proportionné de l'utilisation du régime d'urgence. Tout comme les vingt-quatre heures, ce serait une avancée légère mais nécessaire.

M. le président. Quel est l'avis du Gouvernement sur ce sous-amendement ?

M. Bernard Cazeneuve, ministre. Ce que dit le texte n'est pas ce que dit M. Delarue. Or nous discutons du texte et non de ce que pense M. Delarue, personne par ailleurs tout à fait estimable – et je tiens le plus grand compte de ce qu'il dit.

M. Eduardo Rihan Cypel. Très bien. Il y a matière à un *tweet*...

M. Bernard Cazeneuve, ministre. Mais nous ne votons pas les commentaires de M. Delarue : nous votons un texte. Que dit celui-ci ? Lorsque nous sommes dans une situation d'urgence opérationnelle, le service informe immédiatement le Premier ministre et la CNCTR. Ce n'est pas parce que la CNCTR n'est pas en situation de statuer immédiatement qu'elle n'est pas informée.

Premier élément de réponse : lorsqu'on est en situation d'urgence et qu'il n'est pas possible à la CNCTR de réagir, elle est immédiatement informée, comme le Gouvernement, du recours à telle technique.

Puisque vous disiez que tout se ferait dans le dos du Premier ministre, sachez que celui-ci peut à tout moment demander l'interruption de l'usage de cette technique. Par ailleurs, le service est dans l'obligation de transmettre dans les vingt-quatre heures un document très précis sur les moyens qu'il a mobilisés et les éléments qui l'ont conduit à agir.

Nous nous trouvons donc dans une situation où la CNCTR et le Premier ministre sont prévenus immédiatement, où le Premier ministre peut interrompre à tout moment l'usage de cette technique et où, dans les vingt-quatre heures qui suivent sa mise en œuvre, le service est obligé de transmettre des éléments très circonstanciés à la CNCTR.

M. le président. Quel est l'avis de la commission sur l'amendement du Gouvernement et sur le sous-amendement ?

M. Jean-Jacques Urvoas, rapporteur. Le sous-amendement de M. Tardy a reçu un avis défavorable de la CNCTR...

M. Pascal Popelin. Vous vous voyez déjà la présider ! *(Sourires.)*

M. Jean-Jacques Urvoas, rapporteur. ... de la commission, veuillez m'excuser, parce que la transcription des données collectées ne nous paraissait pas une notion très explicite. En effet, nous considérons que l'article porte sur la géoloca-

lisation en temps réel ou par balise. De manière concrète, leur matérialisation n'est pas apparue de manière évidente à la commission qui a donné un avis défavorable.

En revanche, l'amendement du Gouvernement a été accepté par la commission. Il définit ce que sera demain l'urgence opérationnelle qui permettra soit la mise en œuvre de la géolocalisation en temps réel par données de connexion, y compris par le biais de moyens techniques comme prévu à de l'article 226-3 du code pénal, et la géolocalisation par balise.

(Le sous-amendement n° 412 n'est pas adopté.)

(L'amendement n° 380 deuxième rectification est adopté.)

M. le président. La parole est à M. Jean-Jacques Candelier, pour soutenir l'amendement n° 148.

M. Jean-Jacques Candelier. L'article L. 852-1 du code de la sécurité intérieure prévoit la possibilité d'intercepter les correspondances émises par voie électronique et susceptibles de révéler des renseignements entrant dans les finalités mentionnées à l'article L. 811-3.

Le champ des interceptions de sécurité, régi par la loi de 1991 qui fait référence aux « intérêts publics » listés au nouvel article L. 811-3, est considérablement élargi. En outre, comme le souligne très justement M. Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité, la loi de 1991 prévoit que le recours à cette technique ne peut intervenir qu'« à titre exceptionnel ». Or, ces mots ne figurent pas dans le projet de loi. Les interceptions de sécurité entrent donc dans le cadre normal d'une investigation policière administrative. Pour moi, ce n'est pas acceptable. C'est la raison pour laquelle nous proposons par cet amendement d'introduire dans le texte le caractère exceptionnel des interceptions de sécurité, conformément à la loi de 1991.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Avis défavorable.

(L'amendement n° 148 n'est pas adopté.)

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 43.

M. Sergio Coronado. Je vais le défendre, en effet, et je regrette que mon collègue Popelin ne s'en soit pas inspiré, parce que nous l'avions aussi déposé en commission, monsieur le rapporteur...

Cet amendement vise à préciser que les interceptions de sécurité ne sont possibles que lorsque les renseignements ne peuvent être recueillis par un autre moyen, légalement autorisé. Le retrait du principe de subsidiarité inscrit dans la loi de 1991 nous paraît constituer un recul important.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. J'ai déjà eu l'occasion de le dire, nous ne souhaitons pas que la CNCTR soit le juge de la subsidiarité, qui n'était pas explicitement prévue dans la loi de 1991. L'amendement a donc été repoussé par la commission.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Avis défavorable.

(L'amendement n° 43 n'est pas adopté.)

M. le président. La parole est à M. Jean-Jacques Candelier, pour soutenir l'amendement n° 149.

M. Jean-Jacques Candelier. Le nouvel article L. 852-1 du code de la sécurité intérieure procède à une extension dangereuse des « cibles » d'interception des correspondances émises par voie de communication électronique. Cet article prévoit ainsi la possibilité de suivre des personnes appartenant à l'entourage d'une personne visée par la mesure qui, volontairement ou non, sont susceptibles de jouer un rôle d'intermédiaire pour le compte de cette dernière.

Les expressions « appartenant à l'entourage » et « susceptibles de jouer un rôle d'intermédiaire » sont particulièrement floues et extensives. Il s'agit ici de permettre le placement sur écoute des proches d'une personne au motif, par exemple, que ceux-ci pourraient utiliser son téléphone. Ce dispositif banalise ainsi la surveillance de personnes qui n'ont rien à voir avec l'enquête.

Notons que la CNIL, dans son avis du 5 mars, a émis des réserves sur ce point et que le président de la CNCIS a, quant à lui, souligné le risque d'une trop grande extension de la population couverte par ces techniques.

Cette surveillance, particulièrement intrusive, vise à contourner la jurisprudence de la CNCIS qui exige qu'il existe un lien direct entre la personne placée sur écoute et l'intérêt à protéger.

Pour toutes ces raisons, nous proposons la suppression de la seconde phrase de l'alinéa 35.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Tous nos interlocuteurs, dans la longue liste de ceux que nous avons auditionnés, ont assuré comprendre la nécessité pour les services de renseignement de disposer de moyens d'intervention mais, au fil des entretiens, limitaient les possibilités qui pourraient leur être offertes. Nous finissons toujours pas aboutir à cette question : vous souhaitez que les services soient efficaces mais quels moyens voulez-vous exactement leur donner ?

Un point toutefois faisait l'unanimité : l'extension des interceptions de sécurité à l'entourage, possibilité que M. Candelier propose de supprimer. La commission a donc donné un avis défavorable à son amendement.

J'ajoute que la loi de 1991 permettait d'écouter l'entourage. C'est d'ailleurs grâce à cela que la jurisprudence de la CNCIS a évolué. Considérant l'augmentation du nombre de téléphones, elle a défini la cible non à l'associant à un numéro mais en tant que propriétaire des appareils.

Aujourd'hui, lorsqu'une personne qui représente une menace possède dix téléphones, une seule autorisation est délivrée – ce qui explique qu'en 2014, alors que le quota d'interceptions de sécurité de 2 190 avait été atteint, ce sont en fait 6 600 personnes qui ont été visées.

La jurisprudence de la CNCIS s'est resserrée au fur et à mesure, limitant aujourd'hui les interceptions à un individu et supprimant le lien direct pourtant prévu dans la loi de 1991. Le texte permet une évolution qui nous paraît tout à fait bénéfique.

Ce point ayant été le seul à faire consensus lors des auditions, nous avons donné un avis défavorable à l'adoption de l'amendement de M. Candelier.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

M. le président. La parole est à M. Denys Robiliard.

M. Denys Robiliard. Si je comprends bien les propos de M. le rapporteur, une phrase de l'article L.852-1 visée par M. Candelier casse une « jurisprudence » – si l'on peut employer ce terme – de la CNCIS.

M. Jean-Jacques Urvoas, rapporteur. En effet.

M. Denys Robiliard. Autrement dit, en l'état actuel du droit, ce texte outrepassa le jugement du gardien des libertés, l'institution qu'est la CNCIS, selon quoi une personne est visée mais pas son entourage.

En même temps, on assure que ce projet renforce les libertés alors que le gardien des libertés avait forgé au fil des ans une jurisprudence à l'épreuve des faits considérant qu'il ne fallait pas aller au-delà de la personne visée. Il me semble que l'expérience de la CNCIS doit être prise en compte.

Puisque nous avons connaissance aujourd'hui de sa jurisprudence, qui nous est très loyalement révélée par M. le rapporteur, je propose de la suivre en votant l'amendement de M. Candelier.

M. le président. La parole est à M. le rapporteur.

M. Jean-Jacques Urvoas, rapporteur. Je crains que cet argument ne sonne de manière un peu particulière au regard de ce qu'a montré l'affaire des frères Kouachi, où l'écoute des entourages était interdite.

Je propose donc de repousser l'amendement de M. Candelier mais j'émettrai un avis favorable à l'amendement n° 44 à venir de M. Coronado qui répond largement, si ce n'est dans la lettre, du moins, dans l'esprit, aux préoccupations de M. Robiliard.

(L'amendement n° 149 n'est pas adopté.)

M. le président. Je suis saisi de trois amendements, n° 44, 45 et 46 de M. Sergio Coronado.

Vous pourriez peut-être nous les présenter de manière groupée, monsieur Coronado.

M. Sergio Coronado. Je retire les amendements n° 45 et n° 46 que la commission n'a pas acceptés, l'amendement n° 44 constituant par ailleurs une avancée considérable.

Le rapporteur a dit tout à l'heure qu'il ne souhaitait pas que la CNCTR soit juge de la subsidiarité. Or, comme il rappelle souvent les jurisprudences de la CNCIS, je souhaite quant à moi lui rappeler que, dans son dernier rapport, cette dernière note que les décisions qu'elle prend s'appuient sur les principes de légalité, de proportionnalité et de subsidiarité. Il y a donc une petite évolution regrettable.

S'agissant de l'amendement n° 44, il nous semble important d'encadrer ce qui fonde le soupçon. Actuellement, le projet de loi prévoit que les personnes susceptibles de jouer un rôle intermédiaire, même involontaire, pourront faire l'objet d'interceptions de sécurité. Or, un très grand nombre de personnes peuvent être soupçonnées d'être des intermédiaires involontaires. Compte tenu de l'atteinte à la vie privée que constituent les interceptions de sécurité, il semble nécessaire de préciser cette notion.

Par cet amendement, nous encadrons le soupçon d'être un intermédiaire involontaire car il recouvre un nombre trop important de personnes. Il faudra des indices pour qu'il soit fondé. Nous proposons donc de limiter la surveillance aux personnes qui jouent ce rôle d'intermédiaire en ajoutant, à la seconde phrase de l'alinéa 35, après le mot « Lorsqu' », les mots « il existe des raisons sérieuses de croire qu' ».

(Les amendements n° 45 et 46 sont retirés.)

M. le président. Quel est l'avis de la commission sur l'amendement n° 44 ?

M. Jean-Jacques Urvoas, rapporteur. J'ai indiqué par anticipation que la commission y est favorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 44 est adopté.)

M. le président. La parole est à M. Philippe Folliot, pour soutenir l'amendement n° 122.

M. Philippe Folliot. La rédaction du nouvel article L. 852-1 permet d'autoriser des interceptions de correspondance échangées par des personnes appartenant à l'entourage de la personne visée lorsqu'elles sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour son compte, ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation. Au regard du caractère particulièrement intrusif de cette surveillance, des garanties spécifiques devraient être prévues.

Cet amendement propose de limiter cette possibilité à l'entourage susceptible de jouer un rôle d'intermédiaire volontaire pour le compte de la personne visée et donc de supprimer les mots « ou non » à la deuxième phrase de l'alinéa 35. En revanche, lorsqu'il s'agit de prévenir un acte de terrorisme, le rôle volontaire de l'entourage ne serait pas exigé.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé l'amendement de M. Morin, cosigné par M. Folliot qui vient de le défendre, car il risque d'entraîner une lourdeur administrative au détriment de l'opérationnalité de nos services.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 122 n'est pas adopté.)

M. le président. La parole est à Mme Isabelle Attard, pour soutenir l'amendement n° 189.

Mme Isabelle Attard. Cet amendement vise à ce que les modalités de centralisation des interceptions ne soient définies qu'après avis de la CNCTR. Afin d'assurer un contrôle efficace, il est en effet indispensable que la CNCTR puisse donner son avis sur les modalités de centralisation. L'accès réel aux transcriptions et aux données est l'un des points fondamentaux d'un contrôle efficace, comme l'a rappelé à plusieurs reprises le président de la CNCIS.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a donné un avis favorable à l'adoption de cet amendement de M. Coronado puisqu'il permet de clarifier la situation. Même si, sans son adoption, la CNCTR pourrait faire des recommandations au Premier ministre, le formuler explicitement clarifie sans doute le texte.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(*L'amendement n° 189 est adopté.*)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 414.

M. Lionel Tardy. Lorsque je dis que cette loi est labyrinthique, nous en avons là encore un exemple flagrant. En fait, on refait entrer par la fenêtre les IMSI-catchers et dispositifs assimilés, ce qui est très subtil voire, pardonnez-moi, pernicieux. Je m'explique.

Quelques alinéas plus tôt, nous avons autorisé les dispositifs techniques visés à l'article L. 226-3 du code pénal : interceptions de correspondance, captation de conversations, enregistrement de données informatiques. Après ces derniers, cette autorisation ne valait que pour des données de connexions visées au futur article L. 851-1.

Ici, nous découvrons au détour d'un alinéa sur la centralisation des données que des correspondances pourront aussi être interceptées par ces dispositifs techniques, dont nous connaissons tous le caractère intrusif. Ce sera certes de manière exceptionnelle mais cela ne me suffit pas. Je propose donc de supprimer la possibilité de l'interception de correspondances par ce biais car nous en sommes arrivés à un point où, sauf erreur, le régime d'autorisation et les objectifs de ces appareils ne sont plus clairs du tout. Il ne me semble pas que nous ayons autorisé explicitement cela auparavant.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable par cohérence.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(*L'amendement n° 414 n'est pas adopté.*)

M. le président. La parole est à Mme Isabelle Attard, pour soutenir l'amendement n° 190.

Mme Isabelle Attard. Le recours à l'IMSI-catcher pour intercepter des correspondances portant gravement atteinte aux libertés individuelles du fait de son caractère extrêmement intrusif et totalement non-discriminant concernant les

personnes surveillées, il est indispensable de le limiter à la prévention des actes de terrorisme. C'est d'ailleurs ce que prévoyait le texte initial du Gouvernement.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable pour les raisons que j'ai expliquées tout à l'heure, vu notamment l'encadrement prévu par la commission des lois qui assimile l'usage d'un dispositif technique en interception de correspondances à une interception de sécurité. Le niveau de garantie ainsi accordé permet de ne pas limiter cet usage à cette seule finalité. La commission a repoussé cet amendement.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Sagesse, cet amendement proposant de revenir à une préoccupation initiale du Gouvernement qui n'a pas été suivie par la commission.

(*L'amendement n° 190 n'est pas adopté.*)

M. le président. La parole est à Mme Isabelle Attard, pour soutenir l'amendement n° 191.

Mme Isabelle Attard. Dans la même logique, nous souhaitons que le recours à l'IMSI-catcher pour intercepter des correspondances ne puisse être effectif que sur l'avis conforme de la CNCTR – je présenterai tout à l'heure un amendement de repli n° 192.

Monsieur le rapporteur, l'IMSI-catcher permettant de capter toutes les communications dans un périmètre précis, comment pouvez-vous être certain qu'il n'interceptera que les communications visées puisqu'il interceptera et enregistrera tout ce qui passera à sa portée ?

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable.

Une fois de plus, cet amendement est un moyen de faire en sorte que les avis de la CNCTR soient conformes, ce qui ne correspond pas au point de vue de la commission des lois.

Cependant, en l'espèce, cette mention s'insère après une phrase précisant que le Premier ministre définit les modalités de la centralisation des interceptions de correspondances. Dès lors, on ne comprend pas très bien à quel avis du président de la CNCTR il est fait référence. En toute hypothèse, l'outil devra être employé conformément à l'autorisation accordée. Avis défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(*L'amendement n° 191 n'est pas adopté.*)

M. le président. Sur l'article 2, je suis saisi par le groupe écologiste d'une demande de scrutin public.

Le scrutin est annoncé dans l'enceinte de l'Assemblée nationale.

La parole est à Mme Isabelle Attard, pour soutenir l'amendement n° 192.

Mme Isabelle Attard. Le recours à l'IMSI-catcher pour intercepter des correspondances étant une technique extrêmement attentatoire aux libertés individuelles – je le rappelle

et le martèle, mais ce n'est pas grave – par son caractère extrêmement intrusif et totalement non-discriminant, il est indispensable qu'il soit expressément autorisé, comme le prévoyait d'ailleurs le projet de loi initial.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La rédaction de l'article L.852-1 du code de la sécurité intérieure dans le texte de la commission ne distingue pas entre une interception de sécurité classique et une interception de correspondances réalisée par un dispositif s'agissant du régime d'autorisation. Nous considérons donc que l'amendement est satisfait. Il a été repoussé par la commission.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 192 n'est pas adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 61.

M. Lionel Tardy. Cet amendement de repli propose que les correspondances interceptées de cette façon et sans rapport avec l'enquête soient détruites sans délai, sur-le-champ. Le risque est trop grand pour que l'on se permette une imprécision. Je crois que c'est le sens de la rédaction actuelle, mais il faut le dire plus explicitement : la destruction doit être immédiate.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Cet amendement a été repoussé par la commission, car nous considérons que sa rédaction aboutirait paradoxalement à ce que l'on empêche la destruction des données incidentes qui sont captées par un dispositif technique.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 61 n'est pas adopté.)

M. le président. La parole est à M. Éric Ciotti, pour soutenir l'amendement n° 69.

M. Éric Ciotti. Cet amendement vise à ne pas limiter par des quotas le nombre d'autorisations délivrées par le Premier ministre – quotas qui existent déjà aujourd'hui pour les interceptions de sécurité autorisées par le Premier ministre après avis de la CNCIS. Il s'agit par là d'offrir davantage de souplesse et de latitude au Premier ministre.

Il est vrai que celui-ci a toute latitude pour augmenter les quotas par arrêtés, et il le fait déjà aujourd'hui, dans le cadre défini par la loi de 1991. Mais je souhaiterais, compte tenu de la situation d'urgence et du danger auquel nous devons faire face, que le Premier ministre puisse intervenir avec plus de souplesse et qu'il ne soit pas contraint de revenir en permanence sur ces quotas, qui peuvent avoir un caractère contraignant et même quelquefois paralyser l'action des services.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé cet amendement, car elle considère au contraire que l'existence d'un quota est un élément de contrôle utile, compte tenu du caractère intrusif d'une interception de

sécurité. Au demeurant, l'existence de ce quota n'a jamais rien empêché, puisqu'il a été relevé cinq fois depuis 1991. Le Gouvernement est d'ailleurs en train de le relever une nouvelle fois, de 2150 ou 2190 à 2500, afin de faire face aux besoins supplémentaires. Aucune urgence opérationnelle n'a jusqu'ici empêché l'application des dispositions de la loi.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 69 n'est pas adopté.)

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 193.

M. Sergio Coronado. Il est retiré.

(L'amendement n° 193 est retiré.)

M. le président. Je mets aux voix l'article 2.

(Il est procédé au scrutin.)

M. le président. Voici le résultat du scrutin :

Nombre de votants	30
Nombre de suffrages exprimés	30
Majorité absolue	16
Pour l'adoption	25
contre	5

(L'article 2, amendé, est adopté.)

Article 3

M. le président. La parole est à M. Lionel Tardy, premier orateur inscrit sur l'article 3.

Je rappelle à tous les orateurs inscrits, même si cela ne va pas renforcer ma popularité, que je leur couperai la parole au bout de deux minutes. *(Sourires.)*

M. Lionel Tardy. L'article 3 comporte deux parties : la première, qui porte sur la sonorisation et la captation d'images – j'y reviendrai par voie d'amendements – et la seconde, sur les mesures de surveillance internationale.

J'aimerais m'arrêter un instant sur cette seconde partie, qui concerne les mesures de surveillance et de contrôle des transmissions émises ou reçues à l'étranger. Il me semble que le contrôle est plus faible ici que sur le reste du texte – beaucoup trop faible. Contrairement à ce que prévoient les articles précédents, tout est ici renvoyé à un décret pris en Conseil d'État après avis de la CNCTR, lequel ne sera pas publié.

C'est léger, trop léger ! Et l'on évacue ainsi un grand nombre de questions touchant aux modalités de contrôle des interceptions de communications électroniques émises ou reçues de l'étranger. Il y a bien des modalités de réclamation, mais il y a aussi un grand trou, et ce manque de contrôle pose un problème de prévisibilité. J'espère que nos débats permettront de dissiper ces fortes inquiétudes.

M. le président. La parole est à M. Jean-Jacques Candelier.

M. Jean-Jacques Candelier. L'examen de cet article intervient alors que des révélations sont faites sur la surveillance massive qui existerait – j'utilise le conditionnel – à l'heure

actuelle en France. Quand je lis la presse, j'en prends et j'en laisse, comme beaucoup d'entre vous, mais je souhaite tout de même obtenir une réponse à mes interrogations.

La plate-forme nationale de cryptage et de décryptement – PNCD – installée pour l'essentiel dans les bâtiments du siège de la DGSE à Paris, disposerait des plus puissants calculateurs de France et intercepterait, puis stockerait, des milliards de données françaises et étrangères. J'ai utilisé le conditionnel jusqu'à présent, monsieur le président, vous êtes témoin, mais le Gouvernement ne peut se contenter de démentir.

Le cadre de ce projet de loi ne traite absolument pas de la PNCD. Si le texte reste en l'état, cette plate-forme restera clandestine et sans contrôle démocratique, pas même *a posteriori* ! Dans la mesure où nous ne pouvons plus déposer d'amendements, un amendement gouvernemental doit d'urgence soumettre la PNCD au contrôle de la Commission de contrôle des techniques de renseignement.

Madame la garde des sceaux, messieurs les ministres de l'intérieur et de la défense, que comptez-vous faire pour limiter la fuite d'informations sur les citoyens français vers l'étranger ? Comptez-vous limiter la quantité de données recueillies et analysées chaque jour par la PNCD ? Comptez-vous soumettre au contrôle de la commission indépendante l'activité de cette plate-forme de cryptage et de décryptement ?

M. le président. La parole est à Mme Isabelle Attard.

Mme Isabelle Attard. Monsieur le ministre de l'intérieur, vous nous avez déclaré que vous étiez certain de la constitutionnalité de la loi dont nous débattons. Nous savons tous ici que seuls les juges peuvent dire le droit, et que seul le Conseil constitutionnel peut déclarer cette loi conforme à la Constitution de notre république.

Lorsque Pouria Amirshahi a suggéré que vous défériez vous-même la loi relative au renseignement au Conseil constitutionnel, il n'a pas eu de réponse. C'est, pour le moins, une preuve de la fragilité de vos certitudes. À titre personnel, je suis favorable à une saisine du Conseil constitutionnel sur ce projet de loi relatif au renseignement – l'article 1^{er}, à lui seul, suffit à la justifier. J'espère que d'autres collègues s'y montreront également favorables.

Je me souviens que, sur la loi de programmation militaire, cette saisine avait échoué pour de basses raisons de politique politicienne. Je profite donc de notre débat pour vous annoncer une excellente nouvelle : grâce à la diligence de quelques citoyens éclairés, le Conseil constitutionnel a été saisi ce mardi d'une question prioritaire de constitutionnalité concernant les dispositions liberticides de la loi de programmation militaire. Soyez donc rassurés, chers collègues : si par malchance, ou par inattention, vous deviez voter dans cette loi des dispositions attentatoires à nos libertés publiques et contraires à notre Constitution, les citoyens sauront utiliser tous les moyens à leur disposition pour corriger vos erreurs. Comme le rappelait récemment l'avocat Maître Eolas, dont je vous recommande la lecture, l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 dispose explicitement que la fonction de l'État est la conservation des droits naturels et imprescriptibles de l'homme, à savoir la liberté, la propriété, la sûreté et la résistance à l'oppression.

M. le président. La parole est à M. Philippe Folliot.

M. Philippe Folliot. Nous abordons, avec cet article 3, un point important de ce texte. Notre chère collègue Isabelle Attard vient de poser la question de la constitutionnalité du texte. Chacun et chacun a la liberté de poser une question prioritaire de constitutionnalité, mais le parallèle que vous faites avec la loi de programmation militaire me semble un peu limite, et je tenais à le dire.

Nous sommes à la recherche d'un équilibre entre la nécessité d'assurer la protection de la société et des citoyens et celle de garantir un certain nombre de libertés, notamment la préservation de la vie privée. C'est le grand défi de ce texte, et c'est pour cela que l'UDI proposera une série d'amendements qui visent, sans nuire à l'efficacité des services, à mieux garantir ces libertés, auxquelles nos concitoyens sont très attachés.

M. le président. La parole est à M. Jean Lassalle.

Je rappelle à mon collègue béarnais que, pour lui aussi, le temps de parole est limité à deux minutes – même si je sais qu'il pourrait parler deux heures.

M. Jean Lassalle. Afin de gagner définitivement votre confiance, monsieur le président, je parlerai une minute et cinquante-huit secondes. (*Sourires.*)

Je conseille à nos collègues de ne pas trop en attendre du Conseil constitutionnel, car il n'existe pour ainsi dire plus – et je vous ai fait hier la même démonstration au sujet du Conseil d'État. Et tout cela n'est pas le fruit du hasard : nous avons bradé nos services de l'État, l'un des meilleurs États du monde, au cours de ces quarante dernières années, afin de devenir eurocompatibles. Dans le même temps, depuis dix ans, nous avons démantelé l'organisation de notre territoire, dont il ne reste plus rien.

En ce qui me concerne, je suis d'accord avec cette politique de renforcement du renseignement. Je sais ce qu'il faut faire, mais je n'ai plus confiance. Regardez les préfets : ils sont repolitisés comme il y a cinquante ans. C'est incroyable ! Et ceux qui ne le sont pas ne croient plus à rien. Seuls les gendarmes, et les services de santé, dans une moindre mesure, continuent à bénéficier de l'appui du Premier ministre. Le reste est en désuétude. C'est pour cela que je suis prudent : il faudrait reconstruire l'État avant d'aller plus loin.

J'ai parlé une minute cinquante-huit, monsieur le président !

M. le président. Vous avez même parlé moins que cela. Et comme le préfet des Pyrénées-Atlantiques n'a pas encore déterminé les communes qui sont éligibles à la dotation d'équipement des territoires ruraux, pour ma part, je prendrai sa défense, monsieur le député de la quatrième circonscription. Comme je crois que ses décisions doivent intervenir dans les quinze jours, je lui transmettrai le compte rendu de la séance, pour qu'il lise nos déclarations respectives. (*Sourires.*)

M. Éric Ciotti. C'est du trafic d'influence !

M. le président. La parole est à M. Eduardo Rihan Cypel.

M. Eduardo Rihan Cypel. Monsieur le président, chers collègues, l'article 3 rend légales, tout en leur donnant des délimitations claires, un certain nombre de techniques qui pourraient être utilisées par les services de renseignement dans le cadre administratif. Ces techniques existaient sur le plan judiciaire ; elles existaient probablement aussi, mais sans encadrement juridique, sur le plan administratif. Nous

rendons possible l'utilisation de certaines techniques d'intrusion – balises, sonorisation de lieux privés... – qui sont fondamentales pour l'activité des services, notamment pour anticiper certains événements et identifier des cibles qui voudraient porter atteinte aux intérêts de la nation ou aux intérêts de la France.

Il est important que nous puissions donner à nos services de renseignement ces moyens juridiques et techniques, en les légalisant et en leur donnant un cadre juridique, là où, jusqu'à présent, il n'y avait qu'un vide juridique. Cet article permet de combler ce vide, tout en sécurisant le travail des agents et en définissant, dans la loi, ce que les services de renseignement peuvent faire et ce qu'ils ne peuvent pas faire sur le plan technique, pour remplir les missions qui sont les leurs.

M. le président. La parole est à M. le ministre de la défense.

M. Jean-Yves Le Drian, ministre. Je voudrais seulement apporter deux précisions sur la surveillance des communications internationales, pour répondre aux interventions que je viens d'entendre. Nous aurons peut-être l'occasion d'y revenir lors de l'examen des amendements.

Premièrement, monsieur Candelier, s'agissant du PNCD, il ne faut pas fantasmer exagérément sur le sujet. Son vrai nom est le suivant : Pôle national de cryptanalyse et de décryptement.

Consacré au déchiffrement, c'est-à-dire au traitement des chiffres, il a été créé en 1999. Ce n'est pas une plate-forme et les informations données à ce sujet sont erronées. L'existence de ces capacités de décryptage ou de « décryptement » est implicite dans l'article L. 822-2 du code de la sécurité intérieure tel qu'il résulte de ce projet. Je tenais à vous apporter ces précisions pour lever toute ambiguïté. Je le répète, ce n'est pas une plate-forme mais un outil qui existe déjà depuis un certain temps et qui est nécessaire pour bien maîtriser la surveillance des communications internationales.

Par ailleurs, le présent texte de loi permettra de mettre en œuvre un cadre juridique qui n'existait pas jusqu'à présent puisque la loi de 1991 avait totalement exclu un cadre juridique pour la surveillance des communications internationales. Ce cadre juridique permettra que soit pris un décret classique en Conseil d'État, relatif aux conditions et aux procédures applicables et un autre qui ne sera pas publié mais qui sera soumis à l'avis préalable de la CNCTR ainsi que du Conseil d'État et communiqué à la délégation parlementaire au renseignement. Il ne sera pas publié pour ne pas dévoiler à nos adversaires nos capacités techniques. Le bon sens s'impose en la matière.

Je tenais à apporter ces deux précisions pour éviter toute ambiguïté.

M. le président. Nous en venons aux amendements.

La parole est à M. Jean-Jacques Candelier, pour soutenir l'amendement n° 152.

M. Jean-Jacques Candelier. Le nouvel article L. 853-1 offre aux services de renseignement la possibilité de sonoriser certains lieux et véhicules, ainsi que de capter les images et données informatiques. Il s'agit ainsi de permettre d'écouter et d'enregistrer des conversations, de prendre des photos, y compris dans des lieux privés, et de capter des consultations de sites internet. Le texte fixe une seule condition préalable à l'autorisation d'utilisation de ces techniques : les renseigne-

ments relatifs aux finalités prévues à l'article L. 811-3 ne doivent pas pouvoir être recueillis par un autre moyen légalement autorisé.

Cette condition encadre utilement le recours à ces procédés très intrusifs. Il reste qu'au regard du champ très large des domaines d'application possible de ces techniques et en l'absence d'un réel contrôle préalable, cette disposition paraît insuffisante. Cet amendement vise par conséquent à renforcer l'encadrement de ce dispositif en permettant son autorisation uniquement à titre exceptionnel.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a repoussé cet amendement car le caractère exceptionnel résulte du principe de subsidiarité qui figure explicitement dans l'alinéa en question. Insérer les mots « à titre exceptionnel » ne ferait qu'alourdir la rédaction.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 152 n'est pas adopté.)

M. le président. Je suis saisi de trois amendements, n° 126, 127 et 194, pouvant être soumis à une discussion commune.

La parole est à M. Philippe Folliot, pour soutenir les amendements n° 126 et 127.

M. Philippe Folliot. L'article 3 permet aux services de renseignement d'utiliser de nouvelles techniques de recueil de renseignement jusque-là uniquement dévolues aux services de police judiciaire : la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé ; la captation, la transmission et l'enregistrement de données informatiques transitant par un système automatisé de données ou contenues dans un tel système.

S'il est nécessaire de doter les services de renseignement de techniques similaires à celles dont bénéficient les services de police judiciaire, il convient d'assortir cette possibilité de garanties et de veiller à ce que l'utilisation de ces techniques ne couvre pas un champ trop large.

L'amendement n° 126 vise à en limiter l'utilisation à la seule finalité prévue au 4° de l'article L. 811-3, soit la prévention du terrorisme.

Quant à l'amendement n° 127, il vise à en limiter l'utilisation aux seules finalités prévues aux 1°, 4° et 6° de l'article L. 811-3, soit l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisées.

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 194.

M. Sergio Coronado. Nous avons déposé un amendement similaire à l'article 2 qui avait donné lieu au même débat. Je retire cet amendement car nous avons clos cette discussion par un vote.

(L'amendement n° 194 est retiré.)

M. le président. Quel est l'avis de la commission sur les deux amendements restant en discussion ?

M. Jean-Jacques Urvoas, rapporteur. Pour les mêmes raisons que celles qui conduisent M. Coronado à faire preuve de cohérence en retirant son amendement, la commission a rendu un avis défavorable : pourquoi exclure par principe ces techniques pour des finalités autres que le terrorisme, par exemple les intérêts liés à la politique étrangère qui peuvent recouvrir le respect de certains accords de prohibition ? Dans la mesure où il peut être nécessaire d'utiliser ces outils, cette restriction serait néfaste sur un plan opérationnel.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

M. le président. Monsieur Folliot, retirez-vous vos amendements ?

M. Philippe Folliot. Je retire seulement l'amendement n° 126.

(L'amendement n° 126 est retiré.)

(L'amendement n° 127 n'est pas adopté.)

M. le président. La parole est à M. Philippe Folliot, pour soutenir l'amendement n° 128.

M. Philippe Folliot. Il est défendu.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 128 n'est pas adopté.)

M. le président. Je suis saisi de deux amendements, n° 47 et 129, pouvant être soumis à une discussion commune.

La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 47.

M. Sergio Coronado. Cet amendement vise à préciser les possibilités de captation de données informatiques. La rédaction actuellement prévue va plus loin que les possibilités offertes par l'article L. 706-102-1 du code de procédure pénale, tel qu'issu de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

Il me semblerait incohérent d'autoriser l'utilisation de dispositifs plus intrusifs que ceux autorisés aujourd'hui dans le cadre des enquêtes judiciaires. Cet amendement vise par conséquent à harmoniser les deux rédactions.

M. le président. La parole est à M. Philippe Folliot, pour soutenir l'amendement n° 129.

M. Philippe Folliot. Il est défendu.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission a rendu, là encore, un avis défavorable à ces amendements qui visent à harmoniser le code de procédure pénale et le code de sécurité intérieure, ce qui ne nous semble pas opportun car précisément ceux qui sont chargés d'appliquer le code de procédure pénale le jugent trop restrictif.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(Les amendements n° 47 et 129, successivement mis aux voix, ne sont pas adoptés.)

M. le président. La parole est à M. Éric Ciotti, pour soutenir l'amendement n° 70.

M. Éric Ciotti. Il est défendu.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 70 n'est pas adopté.)

M. le président. La parole est à M. Philippe Folliot, pour soutenir l'amendement n° 137.

M. Philippe Folliot. Cet amendement vise à mieux encadrer le renouvellement du recours aux IMSI-catchers et aux dispositifs dits de proximité. Le projet de loi dispose que l'autorisation sera délivrée pour une durée maximale de deux mois et renouvelable dans les mêmes conditions de forme et de durée que l'autorisation initiale. Cet amendement tend à réduire le délai du renouvellement de deux à un mois.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Nous avons examiné hier soir un amendement presque identique, défendu par M. Morin et que l'Assemblée a repoussé. Par cohérence, nous proposons de repousser celui-ci également.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 137 n'est pas adopté.)

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 195.

M. Sergio Coronado. Cet amendement tend à préciser que le renouvellement de l'autorisation de captation et de sonorisation ne soit possible qu'après avis conforme de la CNCTR.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable. Nous ne souhaitons pas que la CNCTR ait avis décisionnel.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 195 n'est pas adopté.)

M. le président. La parole est à M. Philippe Folliot, pour soutenir l'amendement n° 132.

M. Philippe Folliot. Cet amendement vise à durcir les conditions de renouvellement du recours aux IMSI-catchers et aux dispositifs de proximité. La demande de renouvellement de l'autorisation, à l'issue des deux mois, devra s'accompagner d'un bilan de l'utilisation de ces techniques et des résultats obtenus afin de permettre un avis plus éclairé de la CNCTR.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable. L'amendement est largement satisfait car l'article L. 822-1 prévoit déjà qu'un relevé de chaque mise en œuvre d'une technique de recueil du renseignement est établi, précisant notamment la nature des renseignements collectés. Ce recueil est mis à la disposition de la CNCTR qui peut y accéder à tout moment. De même, l'article L. 822-4 prévoit que les transcriptions et les extractions feront l'objet de relevés tenus à la disposition de la CNCTR.

Ces dispositions étant précises, l'ajout que vous proposez ne paraît pas opportun tout en créant une contrainte inutile pour les services.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 132 n'est pas adopté.)

M. le président. La parole est à M. le rapporteur, pour soutenir l'amendement n° 351 rectifié.

M. Jean-Jacques Urvoas, rapporteur. Cet amendement tend à rendre applicables aux paroles captées dans un lieu privé le délai de conservation prévu au a) du I de l'article L. 822-2.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Avis favorable.

(L'amendement n° 351 rectifié est adopté.)

M. le président. La parole est à M. Jean-Jacques Urvoas, rapporteur, pour soutenir l'amendement n° 350.

M. Jean-Jacques Urvoas, rapporteur. Il est rédactionnel.

(L'amendement n° 350, accepté par le Gouvernement, est adopté.)

M. le président. La parole est à M. Lionel Tardy, pour soutenir l'amendement n° 32.

M. Lionel Tardy. Cet amendement de cohérence avec l'article 1^{er} issu des travaux de la commission vise à ce que le Premier ministre motive sa décision lorsqu'il passe outre un avis défavorable de la commission.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable car l'amendement est satisfait par l'article L. 821-4.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 32 n'est pas adopté.)

M. le président. La parole est à M. Éric Ciotti, pour soutenir l'amendement n° 71.

M. Éric Ciotti. Défendu.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 71 n'est pas adopté.)

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 196.

M. Sergio Coronado. Cet amendement tend à préciser que le renouvellement d'une autorisation d'introduction dans un système de données ne puisse se faire qu'après avis conforme de la CNCTR. Je pense que nous obtiendrons la même réponse que pour l'amendement précédent.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La constance de Sergio Coronado n'a d'égale que la détermination de la commission à ne pas changer sa position. La décision est prise par l'autorité politique et non par l'autorité administrative.

M. le président. Quel est l'avis du Gouvernement ?

M. Bernard Cazeneuve, ministre. Même avis.

(L'amendement n° 196 n'est pas adopté.)

M. le président. Je suis saisi de trois amendements, n° 341, 365 et 342, qui peuvent faire l'objet d'une présentation groupée.

La parole est à M. Jean-Jacques Urvoas, rapporteur, pour les soutenir.

M. Jean-Jacques Urvoas, rapporteur. Tous trois sont rédactionnels.

(Les amendements n° 341, 365 et 342, acceptés par le Gouvernement, sont successivement adoptés.)

M. le président. La parole est à Mme la garde des sceaux, ministre de la justice, pour soutenir l'amendement n° 421

Mme Christiane Taubira, garde des sceaux, ministre de la justice. Il s'agit là d'une sorte de pré-amendement de coordination. Nous allons, à l'alinéa 8 de l'article 4, modifier les conditions du contrôle juridictionnel mais depuis hier nous sommes obligés de revoir certaines dispositions pour tenir compte de cette modification qui interviendra ultérieurement, ce qui est inconfortable.

Cet amendement vise par conséquent à supprimer la référence à une formation de jugement spécialisée du Conseil d'État pour la remplacer par la seule mention du Conseil d'État qui siègera en formation particulière, dont je détaillerai tout à l'heure la composition et la procédure.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La commission n'a pas examiné cet amendement mais par confiance, j'y suis favorable à titre personnel.

(L'amendement n° 421 est adopté.)

M. le président. La parole est à M. Denys Robiliard, pour soutenir l'amendement n° 286.

M. Denys Robiliard. L'amendement adopté à l'article 1^{er} relatif au secret professionnel s'applique-t-il aux techniques relevant de l'article 3 ? Si c'est le cas, je retirerai par cohérence

cet amendement car il n'y a pas de raison de prévoir un régime différent pour la protection du secret professionnel selon l'article dont on relève.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. La réponse à votre question, monsieur Robiliard, est oui.

M. le président. La parole est à M. Denys Robiliard.

M. Denys Robiliard. Par conséquent je retire l'amendement. *(L'amendement n° 286 est retiré.)*

M. le président. La parole est à M. Jean-Jacques Urvoas, rapporteur, pour soutenir l'amendement n° 327.

M. Jean-Jacques Urvoas, rapporteur. Il est rédactionnel. *(L'amendement n° 327, accepté par le Gouvernement, est adopté.)*

M. le président. La parole est à M. Philippe Folliot, pour soutenir l'amendement n° 123.

M. Philippe Folliot. L'article 1^{er} du projet de loi recense de manière limitative les motifs d'intérêt public pour lesquels peut être autorisé le recueil de renseignements par des techniques spéciales prévues par la loi. Parmi ces finalités figuraient dans le projet de loi initial du Gouvernement « les intérêts essentiels de la politique étrangère et l'exécution des engagements internationaux de la France ».

Lors de l'examen du texte en commission des lois, cette finalité a été modifiée pour devenir « les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère ». Cette finalité concernant exclusivement la politique étrangère, un amendement à l'article 1^{er} a visé à la supprimer de la liste des finalités communes à tous les services de renseignement afin de la déplacer.

Le présent amendement tend à inscrire cette finalité à l'article 3 afin qu'elle s'applique exclusivement à l'article L. 854-1 du code de la sécurité intérieure régissant les mesures de surveillance internationale.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Cet amendement n'a pas lieu d'être, cher collègue : il est cohérent avec l'un des amendements que vous avez défendu à l'article 1^{er} et que nous avons rejeté. Il n'y a donc aucune espèce de raison d'adopter celui-ci ; je vous invite à le retirer, faute de quoi j'y serai défavorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Même avis. *(L'amendement n° 123 est retiré.)*

M. le président. La parole est à M. Sergio Coronado, pour soutenir l'amendement n° 48.

M. Sergio Coronado. La dernière phrase de l'alinéa 25 prévoit que la durée de conservation des correspondances interceptées court à compter de la date de leur première exploitation et non de la date de leur collecte.

Il n'y a pas lieu selon moi de prévoir une durée dérogatoire de conservation pour les correspondances échangées à l'étranger, d'autant plus qu'aucune limite n'est prévue. Il est donc proposé de revenir au dispositif de droit commun en respectant les principes défendus par le Conseil d'État, qui a jugé « nécessaire que ce délai commence à courir comme aujourd'hui à compter du recueil des correspondances et non de leur première exploitation ».

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Dans la mesure où l'Assemblée a adopté l'amendement que M. Popelin a défendu à l'article 1^{er} concernant les délais, M. Coronado parle d'or : avis favorable.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Même avis. *(L'amendement n° 48 est adopté.)*

M. le président. Je suis saisi d'un amendement n° 197 qui fait l'objet d'un sous-amendement n° 383.

La parole est à M. Sergio Coronado, pour soutenir l'amendement.

M. Sergio Coronado. Parmi les garanties prévues dans le texte figure le recours devant le Conseil d'État au cas où la CNCTR constaterait une irrégularité dans la mise en place des techniques de renseignement. Néanmoins, cette garantie essentielle disparaît dès lors qu'il s'agit des mesures de surveillance internationale, comme nous l'avons indiqué en commission. L'encadrement de ces mesures de surveillance est pourtant très faible ; en outre, les communications peuvent concerner des personnes se trouvant en France, et les agents bénéficieront d'une immunité renforcée par le présent projet de loi.

Selon nous, si elle constate une irrégularité, la CNCTR ne doit pas seulement remettre un rapport de contrôle au Premier ministre mais aussi pouvoir, le cas échéant, saisir le Conseil d'État selon les modalités définies à l'article L. 821-6 du code de la sécurité intérieure.

M. le président. La parole est à Mme la garde des sceaux, pour soutenir le sous-amendement n° 383.

Mme Christiane Taubira, garde des sceaux. Le Gouvernement est sensible à la garantie supplémentaire que vous proposez d'introduire, monsieur le député. Cependant, la mesure telle que vous la prévoyez serait de nature à ouvrir un champ trop large de recours possibles. Le Gouvernement vous propose donc de sous-amender votre amendement en limitant cette nouvelle garantie aux cas des correspondances émises ou reçues depuis le territoire national et de leurs données de connexion associées. Si vous acceptez ce sous-amendement, le Gouvernement émettra un avis favorable à votre amendement.

(Le sous-amendement n° 383, accepté par la commission, est adopté.)

(L'amendement n° 197, sous-amendé, accepté par la commission, est adopté.)

M. le président. La parole est à M. Denys Robiliard, pour soutenir l'amendement n° 287.

M. Denys Robiliard. Je le retire.
(L'amendement n° 287 est retiré.)

(L'article 3, amendé, est adopté.)

Après l'article 3

M. le président. La parole est à M. Philippe Nauche, rapporteur pour avis de la commission de la défense nationale et des forces armées, pour soutenir l'amendement n° 314.

M. Philippe Nauche, rapporteur pour avis de la commission de la défense nationale et des forces armées. Cet amendement vise à compléter l'article L. 226-3 du code pénal qui interdit l'utilisation et la promotion d'appareils de captation de données informatiques en y ajoutant la référence à l'article L. 853-1 du code de la sécurité intérieure que ce projet de loi vient de créer.

M. le président. Quel est l'avis de la commission ?

M. Jean-Jacques Urvoas, rapporteur. Avis favorable. Cet amendement contribue à sécuriser ce que l'on appelle les « chevaux de Troie administratifs » et à protéger les systèmes d'information et les libertés de nos concitoyens. Il permettra de soumettre ces « chevaux de Troie administratifs » à la même procédure d'autorisation préalable que les « chevaux de Troie judiciaires ». En effet, l'utilisation de chevaux de Troie par l'autorité judiciaire en application de l'article L. 706-102-1 du code de procédure pénale est soumise à l'autorisation préalable du Premier ministre prise sur le fondement de l'article L. 226-3 du code pénal après avis d'une commission interministérielle présidée par l'Agence nationale de la sécurité des systèmes d'information. À cette occasion, celle-ci s'assure de la fiabilité et de la sécurité du dispositif, et vérifie que les outils n'ont bien pour seules fonctions que celles qui sont décrites par le législateur.

M. le président. Quel est l'avis du Gouvernement ?

M. Jean-Yves Le Drian, ministre. Même avis.
(L'amendement n° 314 est adopté.)

M. le président. La suite de la discussion est renvoyée à la prochaine séance.

2

ORDRE DU JOUR DE LA PROCHAINE SÉANCE

M. le président. Prochaine séance, ce matin, à neuf heures trente :

Discussion, selon la procédure d'examen simplifiée, du projet de loi autorisant la ratification de l'accord entre la République française et l'Union européenne visant à l'application, en ce qui concerne la collectivité de Saint-Barthélemy, de la législation de l'Union européenne sur la fiscalité de l'épargne et la coopération administrative dans le domaine de la fiscalité ;

Discussion, selon la procédure d'examen simplifiée, du projet de loi autorisant la ratification du traité d'extradition entre la République française et la République populaire de Chine ;

Discussion du projet de loi autorisant la ratification de l'accord d'association entre l'Union européenne et la Communauté européenne de l'énergie atomique et leurs États membres, d'une part, et la République de Moldavie, d'autre part ;

Suite de la discussion du projet de loi relatif au renseignement.

La séance est levée.

(La séance est levée, le mercredi 16 avril 2014, à zéro heure cinquante.)

La Directrice du service du compte rendu de
la séance de l'Assemblée nationale

CATHERINE JOLY



Prix du numéro : **3,90 €**
(Fascicules compte rendu et amendements)

