

# ASSEMBLÉE NATIONALE

JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE

**XVI<sup>e</sup> Législature**

SESSION ORDINAIRE DE 2022-2023

Séances du jeudi 1<sup>er</sup> juin 2023

## Compte rendu intégral



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

# SOMMAIRE GÉNÉRAL

---

1<sup>re</sup> séance ..... 5407

2<sup>e</sup> séance ..... 5443

# ASSEMBLÉE NATIONALE

JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE

SESSION ORDINAIRE DE 2022-2023

255<sup>e</sup> séance

## Compte rendu intégral

**1<sup>re</sup> séance du jeudi 1<sup>er</sup> juin 2023**

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

# SOMMAIRE

## PRÉSIDENCE DE MME VALÉRIE RABAULT

### 1. Programmation militaire 2024-2030 (p. 5409)

#### DISCUSSION DES ARTICLES (*suite*) (p. 5409)

##### Article 32 (p. 5409)

Mme Mélanie Thomin

Mme Anne Le Hénanff

M. Ugo Bernalicis

Amendement n° 1269

Mme Sabine Thillaye, rapporteure pour avis de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République

M. Jean-Noël Barrot, ministre délégué chargé de la transition numérique et des télécommunications

Amendements n°s 1121, 1665, 1714, 1727, 1274, 171, 170, 837, 992, 173, 1273, 1658

##### Article 33 (p. 5419)

Mme Clara Chassaniol

Mme Anne Le Hénanff

Amendements n°s 1270, 775, 1275, 1587, 1618, 1626, 1669

Sous-amendement n° 1791

Amendements n°s 174, 1272

##### Article 34 (p. 5422)

Mme Anne Le Hénanff

Amendements n°s 1664, 838, 994, 176, 175, 1670, 847 rectifié, 1634, 1673, 839, 996, 1613, 995, 1037, 1217

#### *Suspension et reprise de la séance* (p. 5430)

##### Article 35 (p. 5430)

M. Philippe Latombe

Mme Anne Le Hénanff

M. Ugo Bernalicis

Amendements n°s 177, 840, 997, 1271, 1047, 178, 1276, 1277, 1614, 1278

#### *Rappel au règlement* (p. 5436)

M. Jean-Louis Thiériot

##### Article 35 (*suite*) (p. 5436)

Amendements n°s 179, 180

##### Article 35 *bis* (p. 5437)

M. Philippe Gosselin

M. Aurélien Lopez-Liguori

M. Philippe Latombe

Mme Anne Le Hénanff

M. Ugo Bernalicis

Amendement n° 1631

### 2. Ordre du jour de la prochaine séance (p. 5442)

# COMPTE RENDU INTÉGRAL

## PRÉSIDENTE DE MME VALÉRIE RABAULT

### vice-présidente

**Mme la présidente.** La séance est ouverte.

*(La séance est ouverte à neuf heures.)*

1

## PROGRAMMATION MILITAIRE 2024-2030

### Suite de la discussion d'un projet de loi

**Mme la présidente.** L'ordre du jour appelle la suite de la discussion du projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (n<sup>os</sup> 1033, 1234 rectifié).

### DISCUSSION DES ARTICLES

*(suite)*

**Mme la présidente.** Hier après-midi, l'Assemblée a poursuivi la discussion des articles du projet de loi, s'arrêtant à l'article 32, sur lequel plusieurs orateurs sont inscrits.

### Article 32

**Mme la présidente.** La parole est à Mme Mélanie Thomin.

**Mme Mélanie Thomin.** Au moment d'aborder l'examen du chapitre V relatif au renforcement de la sécurité des systèmes d'information, je tiens à rappeler la démarche du groupe Socialistes et apparentés.

Nous discutons des articles 32 à 36 sous le regard vigilant du Conseil constitutionnel. Lors des débats en commission des lois, l'un de mes amendements, défendu au nom du groupe Socialistes et apparentés – amendement essentiel à ce volet de la loi de programmation militaire (LPM) – a été adopté. Il exige l'assermentation des agents de l'Agence nationale de la sécurité des systèmes d'information (Anssi), assermentation qui ne figurait pas dans le texte initial. Ces agents recueillent des données auprès des acteurs numériques et leur assermentation est nécessaire pour exercer cette fonction sensible. Nous nous félicitons que le texte apporte cette garantie.

En tant que législateur, nous tenons à affirmer le niveau d'exigence et de garantie auquel nous sommes particulièrement attachés. Les articles 32 à 36 visent à renforcer les pouvoirs de l'autorité de contrôle, ce qui est une bonne

chose, mais ce renforcement suppose un cadre équilibré fixant les limites que devra observer l'administration dans le plus strict respect des droits et des libertés.

Dans un contexte d'explosion des attaques cyber, nous sommes favorables à l'élargissement des pouvoirs de l'Anssi pour anticiper et contrer ces attaques, mais nous tenons aussi à poursuivre le travail engagé en commission des lois afin de fixer des garanties imposant à l'administration d'agir dans un cadre strict et délimité et de nous assurer que la loi que nous votons respecte la Constitution.

**Mme la présidente.** La parole est à Mme Anne Le Hénanff.

**Mme Anne Le Hénanff.** Le groupe Horizons et apparentés est favorable à cet article qui permet à l'Anssi, en cas de menace susceptible de porter atteinte à la sécurité nationale, de prescrire plusieurs réponses graduées affectant les noms de domaines, en particulier leur blocage, leur suspension et leur redirection vers un serveur sécurisé ou neutre contrôlé par l'Anssi.

En commission, nous n'avons pas émis de réserve sur cet article, mais nous avons demandé des précisions sur son périmètre d'application. Nous avons présenté un amendement visant à exclure les bureaux d'enregistrement, dont la vocation est commerciale, de l'application de l'article 32, pour réserver celle-ci aux offices d'enregistrement, qui disposent déjà des moyens de mettre en œuvre les dispositions prévues. Nous avons finalement retiré l'amendement après les explications de Mme la rapporteure.

Nous nous réjouissons des modifications apportées en commission, telle que la prise en compte par l'Anssi de la nature du titulaire et de ses contraintes opérationnelles. L'abaissement du délai de conservation des données à cinq ans, au lieu de dix, et la fixation à deux jours ouvrés du délai d'exécution par les opérateurs des mesures prises par l'Anssi semblent être de bonnes choses. Il nous a également paru important que le décret d'application du présent article soit pris après avis de la Commission nationale de l'informatique et des libertés (Cnil).

Pour toutes ces raisons, le groupe Horizons et apparentés votera l'article ainsi rédigé, puisque nous n'avons pas jugé utile de déposer de nouveaux amendements en séance.  
*(M. Lionel Royer-Perreaut applaudit.)*

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Je suis très sceptique sur la portée de l'article 32 et sur les nouvelles prérogatives qu'il donne à l'Anssi. Nous avons eu un petit débat en commission, mais il n'a pas été suffisant pour fournir les éclairages nécessaires à l'évaluation de cet article par rapport à d'autres dispositifs en vigueur.

Nous avons proposé de porter à soixante-douze heures le délai d'exécution des mesures prises par l'Anssi qui, comparé à celui de quarante-huit heures prévu pour contester un référé

liberté, nous a semblé être un minimum. C'est finalement le délai de deux jours ouvrés qui a été retenu. Dans ces conditions, il est préférable de déposer un recours devant le tribunal administratif le vendredi afin de bénéficier d'un jour supplémentaire pour faire valoir ses droits... Je vois que cela faire sourire M. le ministre délégué, mais nous en sommes réduits à devoir faire des boutades pour appeler l'attention sur un sujet qui touche pourtant aux libertés fondamentales.

Depuis les débats en commission, j'ai eu l'occasion de lire des articles sur le fonctionnement actuel de l'Anssi. Il existe des plateformes régionales pour signaler des problèmes, mais la sous-traitance, la concurrence et les embrouilles au sein même de l'Anssi en région et de ses partenaires ne facilitent pas les choses. Ces plateformes destinées aux très petites entreprises (TPE) et aux petites et moyennes entreprises (PME) servent à renvoyer les personnes privées vers d'autres personnes privées proposant des services de sécurité. L'Anssi se contente donc de faire le passe-plat. Il manque encore deux ou trois garanties à un dispositif qui entend donner des prérogatives plus larges à une agence gouvernementale cantonnée à ce rôle pour le respect de l'État de droit et des libertés fondamentales, notamment celles des détenteurs d'URL et de noms de domaine.

Je ne suis pas convaincu, à ce stade, de la pertinence de l'article 32. J'attends donc des réponses de la part du Gouvernement.

**Mme la présidente.** Nous en venons aux amendements.

La parole est à M. Jérémie Iordanoff, pour soutenir le n° 1269.

**M. Jérémie Iordanoff.** L'article 32 dans sa rédaction actuelle confie à l'Anssi des prérogatives en matière de filtrage de noms de domaine dans les cas de menaces susceptibles de porter atteinte à la sécurité nationale. Cette dernière notion est très évasive. Les prérogatives de l'Anssi se trouveraient donc d'autant plus étendues que leur impact sur la liberté d'accéder aux services de communication serait fort.

Il faut donc préciser – c'est la moindre des précautions – les finalités pour lesquelles ces prérogatives peuvent être employées. Nous proposons donc de circonscrire l'application de l'article 32 aux seuls cas où la menace est susceptible de porter atteinte aux intérêts fondamentaux de la nation et de sécuriser cette rédaction en renvoyant à l'article 410-1 du code pénal qui précise que les intérêts fondamentaux de la nation sont ceux « de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel. »

Cette rédaction, différente de celle que j'avais proposée en commission puisqu'on m'y avait opposé que le renvoi au code de la sécurité intérieure n'était pas pertinent, est plus précise. Un consensus s'était dégagé en commission sur la nécessité d'établir une liste de cas précise, la notion de sécurité nationale étant trop vague.

**Mme la présidente.** La parole est à Mme Sabine Thillaye, rapporteure pour avis de la commission des lois constitutionnelles, de la législation et de l'administration générale de la

République, à laquelle la commission de la défense nationale et des forces armées a délégué l'examen des articles 32 à 36, pour donner l'avis de la commission.

**Mme Sabine Thillaye, rapporteure pour avis de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République.** Nous avons évoqué ce sujet en commission. Je comprends tout à fait le sens de votre amendement. Notre objectif est d'être suffisamment large tout en étant précis afin de permettre à nos lois de faire face au plus grand nombre possible de situations compliquées et donc de vivre dans le temps. Or votre rédaction ne permet pas nécessairement de couvrir les cibles privilégiées des cyberattaques que sont les hôpitaux ou les collectivités territoriales.

Légistiquement, votre amendement procède à un mélange de genres qui n'est pas bienvenu. L'Anssi est un service de cybersécurité et de cybersécurité, elle n'est pas un service de renseignement. Nous faisons encore trop souvent cet amalgame, y compris en commission. L'Anssi n'a donc pas vocation à suivre les personnes. Son rôle est d'identifier les victimes d'attaques et de faire face aux situations compliquées provoquées par ces attaques.

Dans un souci d'harmonisation de la rédaction des articles, la formulation actuelle faisant référence aux menaces susceptibles de porter atteinte à la sécurité nationale est préférable à celle proposée par l'amendement. J'émet donc un avis défavorable.

**Mme la présidente.** La parole est à M. le ministre délégué chargé de la transition numérique et des télécommunications, pour donner l'avis du Gouvernement.

**M. Jean-Noël Barrot, ministre délégué chargé de la transition numérique et des télécommunications.** Je salue la qualité des travaux en commission des lois. Ils ont permis d'affiner considérablement la rédaction des articles 32 et suivants. Je pense aux délais opérationnels de mise en œuvre – sur lesquels M. Bernalicis vient de s'exprimer –, à la durée de conservation des données non identifiantes, qui est passée de dix à cinq ans ou à la nécessité de recueillir l'avis de la Cnil préalablement à la publication du décret d'application de l'article. J'adresse donc mes remerciements à toutes les personnes impliquées dans ces travaux.

Je souhaite compléter les propos de Mme la rapporteure pour avis sur cet amendement. La notion d'intérêts fondamentaux de la nation est prévue par le code pénal alors que l'Anssi n'a pas de pouvoirs d'enquête dans ce domaine. La référence au code pénal est donc de nature à entretenir une confusion. J'ajoute que cette notion couvre un spectre plus large que celle de sécurité nationale puisqu'elle englobe par exemple la sauvegarde du patrimoine culturel. L'adoption de l'amendement élargirait donc considérablement la portée de l'article.

Je rappelle, pour rassurer la représentation nationale, que le concept de sécurité nationale a été sanctionné par le Conseil constitutionnel, à l'occasion de l'examen d'une question prioritaire de constitutionnalité (QPC) sur la loi du 1<sup>er</sup> août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, dite loi 5G, comme étant suffisamment précis. Ce concept nous semblant receler toutes les précisions nécessaires, j'émet un avis défavorable sur l'amendement.

*(L'amendement n° 1269 n'est pas adopté.)*

**Mme la présidente.** L'amendement n° 1121 de Mme Emmanuelle Ménard est défendu.

*(L'amendement n° 1121, repoussé par la commission et le Gouvernement, n'est pas adopté.)*

**Mme la présidente.** La parole est à M. Mounir Belhamiti, pour soutenir l'amendement n° 1665.

**M. Mounir Belhamiti.** Il vise à élargir le champ d'application de l'article 32 aux fournisseurs de résolution de noms de domaine définis à l'article 33 du présent projet de loi dans leur globalité, sans limiter sa portée aux seuls hébergeurs et fournisseurs d'accès à internet (FAI). En effet, en l'état actuel de la rédaction, les personnes qui fournissent des navigateurs internet ne sont pas incluses dans le dispositif. Il en est de même pour les fournisseurs de systèmes d'exploitation mentionnés au 10<sup>o</sup> ter de l'article L. 32 du code des postes et des communications électroniques.

Le présent amendement permettrait par conséquent d'inclure dans le champ de l'article les navigateurs et systèmes d'exploitation qui réalisent le processus de résolution des noms de domaine. Il répond ainsi à un objectif de clarification rédactionnelle, de cohérence vis-à-vis du droit positif et d'inclusion de tous les acteurs impliqués dans la sécurisation du système de noms de domaine (DNS). Il permet ainsi de rendre le dispositif plus effectif.

Je précise que notre collègue Bothorel a rédigé cet amendement avec le concours des services de l'Anssi. Je profite de l'occasion qui m'est offerte pour saluer son travail et pour vous prier d'excuser son absence.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** La rédaction proposée par l'amendement complète utilement l'article 32 en donnant une portée plus large aux mesures de blocage. Avis favorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Il introduit une clarification très utile qui permet de renforcer l'efficacité du dispositif. Avis favorable également.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Nous n'avons pas été pleinement rassurés sur les garanties du dispositif dont cet amendement vise à élargir la portée. J'y suis donc opposé car je pense qu'il est préférable d'expérimenter les exceptions au droit commun et les prérogatives exorbitantes de l'Anssi prévues par l'article sur un périmètre sécurisé.

Madame la rapporteure pour avis, vous nous expliquiez tout à l'heure que la mesure vise à défendre les hôpitaux et ainsi de suite. J'en déduis qu'actuellement nous ne les défendons pas,...

**Mme Clémence Guetté.** Ce n'est pas faux !

**M. Ugo Bernalicis.** ...qu'aucun dispositif n'existe, que nous regardons simplement les attaques se dérouler sans agir, que l'Anssi n'a aucune prérogative et les services de renseignement non plus.

Votre précision selon laquelle l'Anssi n'est pas un service de renseignement nous a d'ailleurs fait sourire : c'est vrai, mais nous espérons que ces structures collaborent – du moins que

des canaux de communication existent entre elles –, car les services de renseignement sont bien informés en matière de cyberattaques.

Certes, le Conseil constitutionnel a jugé avec largesse que la notion de sécurité nationale était suffisamment précise. Mais cette institution n'exerce pas – ou en tout cas plus depuis longtemps – un contrôle maximaliste ; elle est plutôt favorable à l'octroi d'un maximum de prérogatives au Gouvernement, pour qu'il ait les mains libres – tant que les incompétences négatives ne sont pas trop nombreuses.

Quant à nous, nous sommes en droit d'examiner de près la portée des mesures administratives attentatoires aux libertés dont il est question à cet article – même si elles sont constitutionnelles en l'état de la V<sup>e</sup> République. Il ne suffit pas de tirer argument de l'autorité d'une décision du Conseil constitutionnel sur une QPC pour clore la discussion – « circulez, il n'y a rien à voir ! » – et étendre le périmètre de l'article, comme le prévoit cet amendement.

En l'état, je ne voterai pas celui-ci, faute d'éléments suffisants – y compris dans l'étude d'impact – sur ce qu'interdit le droit en vigueur et ce qu'autorisera ce dispositif élargi.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** En commission des lois, nous avons débattu des moteurs de recherche. Les membres du groupe Démocrate ont regretté qu'ils ne soient pas visés par cet article – c'était peut-être notre seul bémol à son propos.

L'extension du dispositif prévue dans cet amendement est donc bienvenue. Nous le savons très bien, depuis quelques semaines, quelques mois, les navigateurs connaissent une importante évolution technologique, en intégrant l'intelligence artificielle. Les attaquants pourront s'en saisir pour mieux jouer des failles. Il faut donc absolument élargir les prérogatives de l'Anssi, comme le prévoit l'amendement.

Monsieur Bernalicis, nous l'avons déjà dit, les modifications apportées en commission des lois aux premiers alinéas de l'article 32 nous conviennent. En outre, pour répondre à votre objection, la décision du Conseil constitutionnel sur la loi « 5G » sécurise leur rédaction – nous n'avons donc plus de réserve sur ceux-ci.

Quant à l'amendement, nous le soutenons également car il faut absolument donner à l'Anssi les moyens de prévenir les menaces qui apparaîtront dans les prochaines semaines à la suite des évolutions technologiques des navigateurs, notamment pendant les Jeux olympiques. Alors qu'en commission des lois, nous, membres du groupe MODEM, souhaitons plutôt restreindre le champ de cet article, les modifications apportées et la décision du Conseil constitutionnel nous ont rassurés et nous sommes donc favorables ici à son extension.

*(L'amendement n° 1665 est adopté.)*

**Mme la présidente.** Je suis saisie de deux amendements identiques, n° 1714 et 1727.

La parole est à M. Ugo Bernalicis, pour soutenir l'amendement n° 1714.

**M. Ugo Bernalicis.** Revenons-en d'abord à l'extension du dispositif, que nous venons d'adopter. Il est extraordinaire que le Gouvernement, dans le projet de loi initial, n'ait pas été capable de préciser que la mesure visait les moteurs de recherche, alors qu'il travaille en lien avec les services de

l'Anssi ! Cela devrait suffire à nous alerter : des débats internes ont sans doute eu lieu sur le caractère sensible – *touchy* – de la mesure ou sur sa nécessité.

Venons-en au délai prévu pour que nos concitoyens fassent valoir leurs droits quand l'administration n'est pas dans son bon droit, précisément – soit qu'une erreur ait été commise, soit qu'il s'agisse d'un recours de principe. Le délai initialement prévu, de vingt-quatre heures, me semblait choisi pour coïncider avec celui en vigueur fixé dans la loi par les macronistes pour demander aux plateformes de retirer des *fake news*.

Ensuite, puisqu'il s'agit de l'intérêt de la nation, je me suis demandé pourquoi vous n'aviez pas repris le délai d'une heure accordé aux plateformes pour supprimer les contenus terroristes aux termes de la loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne, à laquelle j'étais d'ailleurs opposé et sur laquelle j'ai saisi le Conseil constitutionnel. Tout de même, il s'agit de la sécurité nationale, des hôpitaux et ainsi de suite, c'est énorme !

Finalement, vous avez porté le délai de vingt-quatre heures à quarante-huit heures ouvrées. Pourtant, le délai le plus logique, le plus cohérent, aurait été celui de soixante-douze heures pour faire un recours devant le tribunal administratif. J'aimerais comprendre le raisonnement qui vous a conduits à choisir ces délais – et non celui d'une heure. En avez-vous décidé à pile ou face ? S'agissait-il de couper la poire en deux ? Je sais que les décisions sont parfois prises ainsi sur un coin de table – nous ne sommes pas complètement naïfs sur la manière dont les normes sont fabriquées dans notre pays – c'est d'ailleurs ainsi qu'a été décidée la règle des 3 % pour le traité de Maastricht. Après tout, pourquoi pas ? Enfin, je souhaiterais que le délai soit porté à soixante-douze heures, pour apporter des garanties supplémentaires.

**Mme la présidente.** L'amendement n° 1727 de M. Aurélien Saintoul est défendu.

Quel est l'avis de la commission sur ces amendements identiques ?

**Mme Sabine Thillaye, rapporteure pour avis.** Nous essayons à chaque fois de trouver une position équilibrée. Après avoir auditionné, entre autres, les représentants des opérateurs, ceux de nos structures administratives et ceux de l'Anssi, nous avons placé le curseur à quarante-huit heures ouvrées, ce délai paraissant le plus pertinent pour faire face à des situations compliquées, sans pour autant alourdir la charge des opérateurs. Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Le Gouvernement n'a pas la science infuse (*Sourires sur les bancs du groupe LFI-NUPES*) ; ses textes s'enrichissent donc des discussions qui ont lieu à l'Assemblée et au Sénat. Rectifions simplement un fait : le délai initialement prévu était non de vingt-quatre mais de quarante-huit heures, le même, du reste, que celui prévu par la loi pour le retrait des *fake news* – soit un délai plus long que celui de vingt-quatre heures alloué aux hébergeurs, après injonction des forces de l'ordre, pour le retrait des contenus terroristes et pédopornographiques.

Des raisons opérationnelles ont motivé tant le choix du délai initial, qui s'est révélé problématique, que celui, effectué en commission, de l'assouplir, en tenant compte des jours ouvrés. C'est le compromis trouvé en commission, derrière lequel le Gouvernement se range.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Certes, le Gouvernement, comme beaucoup de monde, n'a pas la science infuse.

**M. Laurent Jacobelli.** Contrairement à M. Bernalicis !

**M. Ugo Bernalicis.** Toutefois, il peut s'appuyer sur les services à sa disposition, qui, normalement, dans le cadre de l'étude d'impact, notamment, anticipent les choses, présentent un état du droit, ainsi que les changements, les améliorations, qu'apportera le texte – hélas, en l'occurrence, les paragraphes de l'étude d'impact consacrés à l'article 32 ne clarifient pas les points dont nous sommes en train de discuter.

Si je suis le raisonnement de Mme la rapporteure pour avis, vous avez choisi en commission une position d'équilibre, pour prendre en considération tant les plaintes des opérateurs – « le délai est trop court, il faudra ajouter des moyens, embaucher ; d'accord, puisqu'il s'agit de la sécurité nationale, mais enfin vous êtes pénibles » – que les alertes de personnes comme nous sur la nécessité de prévoir des délais suffisants pour les recours car nous sommes dans un État de droit – encore un peu, du moins.

Or, par-delà cette question d'équilibre, je vous interrogeais sur votre logique. S'il s'agit de contenus des plus problématiques ou d'attaques visant un hôpital, par exemple, je serais moi-même prêt à admettre que des délais de soixante-douze heures ou de quarante-huit heures ouvrées sont trop longs. Mais peut-être que les menaces visées ne sont pas si graves, qu'elles sont déjà bien anticipées, que l'action des services de l'Anssi est seulement entravée par le manque de moyens humains, que des effectifs supplémentaires tant dans cette agence que chez les opérateurs permettraient des délais beaucoup plus rapides que soixante-douze heures.

Choisissons en tout cas un délai logique, qui permette à nos concitoyens de faire valoir leurs droits, dans le cadre d'un État de droit, devant un tribunal administratif, suivant la procédure de référé. Pour ma part, je poursuis une logique, j'argumente ; j'aimerais que vous soyez sur la même longueur d'onde.

**Mme la présidente.** La parole est à Mme Anne Le Hénanff.

**Mme Anne Le Hénanff.** Soyez rassuré : si vous cherchez une logique, celle adoptée dans le texte est simple. Il convient de trouver un délai acceptable pour les deux parties : l'opérateur, en l'occurrence l'Anssi, et sa cible – une personne, une organisation, une entreprise. Nous l'avons évoqué en commission, l'idéal serait effectivement que l'Anssi puisse intervenir en une heure. Elle ne le peut pas,...

**M. Ugo Bernalicis.** Pourquoi ?

**Mme Anne Le Hénanff.** ...car l'organisation ciblée doit avoir matériellement le temps de réagir.

**M. Ugo Bernalicis.** Au fond, vous avez tranché pile entre le milieu et le centre !

(*Les amendements identiques n° 1714 et 1727 ne sont pas adoptés.*)

**Mme la présidente.** La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n° 1274.

**M. Jérémie Iordanoff.** La rapidité ne peut être notre seule préoccupation quand il s'agit, comme ici, du sujet important des libertés fondamentales. Sans revenir sur la nécessité de renforcer les capacités d'intervention de l'Anssi, il faut que l'arsenal juridique respecte les droits et libertés.

Le présent amendement vise à renforcer les droits des personnes visées par les injonctions prises par l'Anssi, en prévoyant qu'elles puissent être en mesure de présenter leurs observations et, le cas échéant, de régulariser leur situation, afin d'éviter qu'à cause de problèmes involontaires, des décisions arbitraires coupent l'accès de certains à l'information sans raison valable.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Ce dialogue est déjà prévu. L'alinéa 2 de l'article prévoit que l'Anssi s'adresse d'abord au titulaire du nom de domaine, avant, en cas de carence de ce dernier, de saisir les fournisseurs d'accès à internet ou les hébergeurs. En commission, nous avons en outre adopté un amendement prévoyant que l'Anssi « tient compte de la nature de ce titulaire ainsi que de ses contraintes opérationnelles ».

Votre amendement pose par ailleurs un problème légistique. Il tend à compléter l'alinéa 10, lequel concerne à la fois les titulaires ayant enregistré leur nom de domaine de bonne foi, avec lesquels un dialogue est prévu, comme je l'ai précisé, et les cyberattaquants ayant enregistré un nom de domaine de mauvaise foi pour orchestrer une attaque. Or, dans ce cas de figure, il ne paraît pas pertinent de demander à l'attaquant de présenter ses observations. Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à M. Aurélien Saintoul.

**M. Aurélien Saintoul.** Poursuivons nos échanges sur les délais. Peut-être est-ce parce que je ne suis pas commissaire aux lois et que je suis novice sur ces sujets, mais cela pique ma curiosité : pourquoi le délai de retrait d'un contenu est-il de vingt-quatre heures quand il s'agit de contenus terroristes ou pédopornographiques, mais de quarante-huit heures quand il s'agit de la sécurité nationale ? Je ne comprends pas la cohérence.

Mme Le Hénanff nous explique que dans l'idéal, le délai de retrait devrait être d'une heure, mais que c'est impossible. Je m'interroge, peut-être bêtement : pourquoi, en matière de sécurité nationale, l'idéal et le standard ne coïncident-ils pas ? (*Mme Clémence Guetté et M. Antoine Léaument applaudissent.*)

Ce serait pourtant normal. C'est peut-être un tropisme de commissaire de la défense, qui place le petit doigt sur la couture du pantalon dès qu'il s'agit d'intérêt national, mais enfin, je trouve curieuse la désinvolture avec laquelle vous acceptez cet écart. Je ne comprends pas la logique.

**M. Antoine Léaument.** Il a raison, ce n'est pas clair !

(*L'amendement n° 1274 n'est pas adopté.*)

**Mme la présidente.** La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n° 171.

**Mme Mélanie Thomin.** Les députés du groupe Socialistes et apparentés entendent subordonner l'exécution de mesures prévues à l'article 32 à l'avis conforme de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). En tant qu'autorité administrative indépendante, celle-ci garantit le respect de nos droits et de nos libertés fondamentales lors de l'application de telles mesures.

Comme évoqué tout à l'heure, notre groupe ne s'oppose pas à l'extension des pouvoirs de l'Anssi, mais souhaite l'accompagner de garanties, dans le respect de l'État de droit. S'il nous faut pouvoir formuler une injonction aux opérateurs afin de sécuriser le contrôle et l'exploitation des systèmes d'information, nous considérons que seul un avis conforme de l'Arcep est en mesure de préserver nos droits et libertés, en contraignant l'administration à les respecter.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Vous souhaitez subordonner l'application des mesures prévues à l'article à l'obtention d'un avis conforme de l'Arcep. Je comprends votre idée, dont nous avons déjà débattu en commission. Toutefois, le dispositif proposé serait particulièrement lourd pour cette agence et devrait donc, à mon avis, être réservé aux cas les plus problématiques en matière de libertés publiques.

C'est pourquoi l'article prévoit que de la redirection du nom de domaine vers un serveur sécurisé de l'Anssi ne peut excéder deux mois, renouvelable une seule fois en cas de persistance de la menace, et après avis de l'Arcep. Cette mesure doit cesser sans délai lorsque la menace est maîtrisée.

Les autres mesures sont également soumises au contrôle de l'Arcep, qui dispose d'un accès permanent aux données collectées par l'Anssi. En outre, toutes les mesures ordonnées par l'Anssi sont susceptibles de recours devant le juge administratif, dans les conditions du droit commun. L'ensemble de ces garanties me paraît suffisant. Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Le débat sur les amendements précédents doit nous permettre de replacer ces mesures administratives dans le panorama des mesures de filtrage existantes – retrait en vingt-quatre heures des contenus terroristes et pédopornographiques. Dans ce dernier cas, le flux est particulièrement élevé puisque, l'an dernier, ce sont 74 000 demandes de retrait de contenus pédopornographiques qui ont été adressées par les autorités aux hébergeurs.

En l'espèce, les atteintes manifestes à la sécurité nationale, visées par les articles dont nous débattons ce matin se chiffrent – ou se chiffreront – à une ou deux dizaines au maximum, la sécurité nationale étant engagée en cas d'attaque coordonnée et massive sur certaines autorités ou certains opérateurs d'importance vitale.

Ainsi, il s'agit d'événements critiques mais dont le nombre est très restreint. C'est pourquoi il faut aussi lire ces articles à la lumière de ces explications, et ne pas comparer ces dispositifs avec d'autres mesures administratives de filtrage.

Mme la rapporteure pour avis a bien exposé les modalités de contrôle de l'Arcep : elle est notifiée dès qu'une demande de filtrage est réalisée, et elle peut s'opposer à la poursuite du filtrage si elle considère qu'il n'est pas approprié. En outre,

l'avis conforme de l'Arcep est nécessaire pour tout renouvellement de la demande. Dans ces conditions, le Conseil d'État a rendu un avis très clair sur cet article : le cadre dans lequel ces demandes de filtrage peuvent être réalisées est proportionné à l'objectif poursuivi.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Vous auriez pu dire que l'Arcep n'a pas les moyens de rendre un avis conforme dans les délais et qu'en conséquence, nous allions nous en passer – mais ce n'est pas un très bon argument, vous me l'accorderez.

Vos longues explications ont le mérite de nous apprendre des choses intéressantes : on parle de deux dizaines d'attaques majeures coordonnées. Enfin, nous commençons à comprendre de quoi il s'agit ! Mais, pour deux dizaines d'attaques par an, nous ne serions pas capables de mobiliser des équipes, à l'Anssi, en mesure de réagir en une heure... Nous en revenons toujours à mes interrogations sur le délai. Il s'agit tout de même d'attaques contre des opérateurs vitaux, d'atteinte à la sécurité nationale – ce sont vos termes, monsieur le ministre délégué.

Vous estimez que, parce qu'il y en a peu, nous avons le temps. Mais la sévérité de l'attaque imposerait au contraire la mise en œuvre d'importants moyens dans un délai très court !

**M. Antoine Léaument.** Exactement !

**M. Ugo Bernalicis.** Dans le cas contraire, nous sommes foutus et n'importe quel hacker va estimer qu'en France, nous sommes vraiment des rigolos – sans doute le sommes-nous eu égard aux moyens affectés à l'Anssi ou à d'autres agences et aux autorités administratives indépendantes chargées de contrôler leur action.

Vous ne pouvez donc vous contenter de brandir les garanties juridiques, formelles, du texte puisque nous savons que, dans les faits, elles ne pourront être mises en œuvre correctement. C'est pourquoi, chacun à notre manière, même si nous savons que ces autorités sont parfois, voire souvent, des lames émoussées, nous essayons de faire en sorte que ce soit mieux que si c'était pire. Ainsi, nos camarades socialistes proposent un avis conforme, garantie supplémentaire.

Mais, même cela, c'est trop pour vous ! Plus nous avançons dans l'examen de cet article, plus j'ai l'impression qu'il est urgent de ne pas donner de telles prérogatives à l'Anssi et d'en rester à l'état actuel du droit, qui permet de faire face aux attaques même si, actuellement, nous ne les empêchons pas...

*(L'amendement n° 171 n'est pas adopté.)*

**Mme la présidente.** La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n° 170.

**Mme Mélanie Thomin.** Il s'agit d'améliorer la lisibilité du texte afin que le juge des référés puisse intervenir, suivant la procédure du référé liberté, sur les décisions prises au titre du présent article. La République doit rester un État de droit en toutes circonstances, même lorsqu'il s'agit de défense nationale.

Nous souhaitons que cette possibilité soit visible dans le texte, pour les opérateurs mais aussi pour tout citoyen, afin qu'il soit en mesure de comprendre la loi. Notre amendement vise donc à rendre la loi plus intelligible.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Le référé liberté est à la disposition de tout justiciable, sous réserve de remplir plusieurs conditions prévues à l'article L. 521-2 du code de justice administrative : l'administration doit avoir porté une atteinte grave à une liberté fondamentale – le juge l'apprécie *in concreto* ; l'atteinte doit être manifestement illégale ; elle doit être imputable à une personne morale de droit public ou à un organisme de droit privé chargé d'un service public ; la requête doit être justifiée par une urgence à agir pour faire cesser cette atteinte.

Si ces critères sont réunis, le recours au référé liberté est possible. Votre demande est donc satisfaite en l'état du droit. En outre, si nous ajoutions une telle précision, il faudrait le faire pour chaque dispositif que nous créons, ce qui alourdirait considérablement nos codes, convenez-en. Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à M. Antoine Léaument.

**M. Antoine Léaument.** Madame la rapporteure pour avis, il est simplement proposé d'ajouter dans la loi que les décisions prises dans le cadre de l'article 32 puissent être soumises au juge administratif suivant la procédure du référé liberté. Il s'agit que nos concitoyens connaissent leurs droits – rien de grave à le rappeler dans la loi, donc. Cela ne coûte rien, ne crée pas de nouvelle dépense, ni de problèmes particuliers. Il s'agit seulement d'un rappel utile car les dispositions que vous proposez pourraient, dans certains cas, attenter aux libertés publiques. Il est donc normal d'effectuer un tel rappel, dans le cas où la loi deviendrait abusive.

J'ai du mal à comprendre pourquoi il est possible de légiférer sur le drapeau européen, mais pas de préciser les droits des citoyens. Ce serait pourtant une mesure efficace.

**Mme la présidente.** La parole est à Mme Sabine Thillaye, rapporteure pour avis.

**Mme Sabine Thillaye, rapporteure pour avis.** Je comprends votre souci d'information du public sur le référé liberté, mais pensez-vous qu'ajouter « le contrôle juridictionnel sur les mesures prises au titre du présent article s'exerce notamment... »

**M. Antoine Léaument.** « Notamment » !

**Mme Sabine Thillaye, rapporteure pour avis.** ...« dans les conditions prévues à l'article L. 521-2 du code de justice administrative » permettra à tous les citoyens de comprendre leurs droits ?

**M. Antoine Léaument.** Oui !

**Mme Sabine Thillaye, rapporteure pour avis.** Il est préférable de se tourner vers un avocat, celui-ci étant parfaitement en mesure de les expliquer à nos concitoyens.

*(L'amendement n° 170 n'est pas adopté.)*

**Mme la présidente.** Je suis saisie de deux amendements identiques, n° 837 et 992.

L'amendement n° 837 de M. Aurélien Saintoul est défendu.

La parole est à M. Ugo Bernalicis, pour soutenir l'amendement n° 992.

**M. Ugo Bernalicis.** Cet amendement vise l'alinéa relatif à la conservation des données, pour une durée initialement prévue de dix ans. En commission – c'est probablement le fruit de l'équilibre entre le centre, le milieu et le centre de gravité –, ce délai est passé à cinq ans, sans qu'on s'interroge sur l'intérêt de conserver ces données. Pourquoi les conserve-t-on? Que va-t-on en faire? Sans réponse à ces questions, nous ne pouvons en déduire un délai logique et devons nous contenter de cet « équilibre ».

Pourquoi le bon équilibre n'est-il pas deux ans, de nombreuses données étant conservées pour deux ans dans différents codes, notamment le code de la sécurité intérieure? Pourquoi pas un mois, délai classique en matière de vidéosurveillance par exemple? Sur quoi s'aligne-t-on? Quel est votre raisonnement? Avez-vous choisi dix ans car il s'agit d'un chiffre rond, puis l'avez-vous divisé par deux parce que les gens ont râlé? Un tel raisonnement me semble un peu limité car il s'agit de données sensibles, la protection de la vie privée et les modalités de conservation des données personnelles faisant partie intégrante de nos droits fondamentaux.

**M. Frank Giletti.** C'est votre raisonnement qui est limité!  
(*M. Laurent Jacobelli acquiesce.*)

**M. Ugo Bernalicis.** Je le répète, nous aimerions comprendre. En commission, nous avons évoqué des délais d'un an et demi, voire de deux ans, pour se prémunir de nouvelles attaques par les mêmes personnes ou organismes. Dont acte, car il s'agit là d'éléments objectifs, liés à ce qu'on sait de ces attaques du fait des retours d'expérience.

A-t-on, aujourd'hui, affaire à des attaquants que nous connaîtrions depuis dix ans, sachant que les technologies d'attaque ont largement changé pendant cette période? Des données numériques, conservées pendant un tel délai, seront complètement obsolètes.

**Mme la présidente.** Merci de bien vouloir conclure.

**M. Ugo Bernalicis.** Je ne comprends pas plus le sens de ces cinq ans, que celui des dix ans...

**Mme la présidente.** Quel est l'avis de la commission?

**Mme Sabine Thillaye, rapporteure pour avis.** Avis défavorable. S'il était adopté, votre amendement reviendrait à supprimer les modalités d'encadrement de la conservation des données recueillies au titre de l'article 32. C'est surprenant de votre part car juridiquement très insécurisant. Ce n'est donc probablement pas votre volonté.

Sans doute s'agit-il d'un amendement d'appel par lequel vous voulez marquer votre opposition aux nouvelles autorisations en matière de collecte de données, sans motif légitime apparent; or l'alinéa 14 concerne les cas où des cyberattaquants ont sciemment exploité un nom de domaine aux fins de porter atteinte à la sécurité nationale. Il s'agit d'obtenir des éléments sur le comportement de l'attaquant, sur son mode opératoire, afin de neutraliser la menace, d'identifier les victimes et de mieux prévenir les attaques.

L'alinéa prévoit des délais de conservation limités, sous le contrôle de l'Arcep. D'ailleurs, dans son avis sur le projet de loi, le Conseil d'État observe que le dispositif envisagé est justifié par la sauvegarde des intérêts fondamentaux de la nation et par la prévention des atteintes à l'ordre public.

J'ai néanmoins souhaité une diminution de la durée de conservation de ces données, de dix à cinq ans. C'est pourquoi je suis opposée à la suppression de l'alinéa 14.

**Mme la présidente.** Quel est l'avis du Gouvernement?

**M. Jean-Noël Barrot, ministre délégué.** L'article 32 permet à l'Anssi de demander le filtrage d'un nom de domaine. À première vue, le lien n'est donc pas évident avec la collecte de données relatives à l'attaque. En réalité, cette dernière peut être décidée si, au moment de demander le filtrage du nom de domaine, l'Anssi réoriente certains flux associés à l'attaque vers un de ses serveurs sécurisés. Ledit serveur va alors percevoir certaines des données relatives à l'attaque, dont le champ sera extrêmement limité. C'est pourquoi le Gouvernement considère que, sur cet article comme sur les suivants, le choix de la commission – cinq ans – est un bon compromis.

À l'article 35, le délai n'a pas été ramené à cinq ans en commission, mais un amendement de Mme Thomin le prévoit. Pour les quatre articles concernés – de l'article 32 à l'article 35 –, cela nous paraît approprié. Avis défavorable.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Vous admettez qu'aucun argument ne vient soutenir le choix de cinq ans, plutôt que celui de dix ans, si ce n'est qu'une durée inférieure est plus protectrice. Pour nous convaincre, des arguments de fond sont nécessaires. Dites « intérêts fondamentaux de la nation » et je suis transi, prêt à conserver les données à vie tant elles sont sensibles puisque touchant à ces intérêts.

**M. Antoine Léaument.** Ça, c'est vrai!

**M. Ugo Bernalicis.** Je suis plus mitigé quand le risque est l'atteinte à l'ordre public, car cette formule peut désigner tout et n'importe quoi. Certains pourraient ainsi considérer que nous porterions atteinte à l'ordre public macronien – ils n'auraient pas complètement tort. Selon eux, nous apporterions même le chaos.

La question est de savoir quelles garanties on détermine. L'alinéa 14 prévoit la destruction immédiate des données personnelles. En cas d'attaque, si vous déroutez le flux de données vers un serveur sécurisé pour le circonscrire et l'analyser, afin d'empêcher l'attaque, vous saisissez tout: toutes les données relatives au nom de domaine concerné seront transférées au serveur sécurisé. S'il s'agit d'un site commercial ou d'un grand groupe, par exemple, les données personnelles des gens qui y travaillent, comme leurs identifiants et leurs mots de passe, seront stockées. Vous prenez certes la précaution d'affirmer que les données personnelles seront détruites. Mais comment? La tâche sera-t-elle confiée à un algorithme ou à un agent? Quelles données seront conservées? Un contrôle sera-t-il réellement effectué et si oui, par qui? L'Arcep a-t-elle les moyens de s'en charger?

Vous nous assurez que tel sera le cas, puisque le texte le prévoit formellement. Mais dans le monde réel, il y aura en vérité des tas de données parmi lesquelles on ne pourra distinguer celles qui sont personnelles: elles seront conservées pendant des années et pourront être utilisées à je ne sais quelles fins. Et nous devrions vous croire sur parole, en faisant confiance à l'action forcément géniale de services qui jamais ne connaîtraient aucune faille? Sur ce dernier point, le petit article qui vient de paraître sur la Commission nationale de contrôle des techniques de renseignement (CNCTR) devrait nous faire réfléchir.

**Mme la présidente.** La parole est à M. le ministre délégué.

**M. Jean-Noël Barrot, ministre délégué.** Ce n'est pas ce que prévoit l'article. Nous avons évoqué la gradation de la mesure. Si le titulaire du nom de domaine est de bonne foi, par exemple une entreprise ou un site comme ceux que vous avez mentionnés, il ne peut y avoir de redirection vers un serveur de l'Anssi. Elle ne sera décidée que si le nom de domaine est détenu par un assaillant ou qu'il a été acquis à des fins malveillantes.

**M. Ugo Bernalicis.** Ça ne répond pas à la question !

*(Les amendements identiques n<sup>os</sup> 837 et 992 ne sont pas adoptés.)*

**Mme la présidente.** La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n<sup>o</sup> 173.

**Mme Mélanie Thomin.** Pourquoi cinq ans ? Lorsque la commission des lois en a débattu, les commissaires de la défense, dont je suis, étaient fort occupés.

**M. Jean-Louis Thiériot.** C'est vrai : ça bosse !

**Mme Mélanie Thomin.** Nous avons su toutefois que Mme la rapporteure pour avis avait rencontré quelques difficultés à justifier le choix d'une conservation des données pendant cinq ans.

La conservation des données n'est pas neutre en ce qu'elle touche aux libertés ; plus on en réduit la durée, mieux le droit se porte. L'amendement vise donc à substituer au mot « cinq » le mot « deux ». Un délai de cinq ans revient à renvoyer aux calendes grecques l'exploitation des données, qui doit être immédiate pour être efficace. Pour assurer une meilleure efficacité de l'administration, nous proposons donc de réduire à deux ans la durée de l'exploitation des données.

**M. Emeric Salmon.** Pourquoi deux ans ?

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Avis défavorable. Vous affirmez que le choix d'un délai de cinq ans, au lieu de dix ans, est arbitraire. Il est le fruit des discussions avec l'Anssi, qui considère qu'il s'agit du temps nécessaire pour effectuer les recherches d'antériorité qui parfois s'imposent. La précédente durée de dix ans était excessive, mais deux ans seraient insuffisants...

**M. Antoine Léaument.** Ce serait trop court, ah bon ?

**Mme Sabine Thillaye, rapporteure pour avis.** ...pour comprendre le mode opératoire.

Nous cherchons toujours l'équilibre entre l'efficacité et la protection des libertés : c'est bien plus difficile que de défendre des avis tranchés. *(Applaudissements sur les bancs des groupes RE, Dem et HOR.)*

**Mme Clémence Guetté.** C'est bien d'avoir des avis, tout de même !

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Mme la rapporteure pour avis a très bien argumenté. J'ajoute que dans certains cas avérés, les assaillants ont repris des architectures d'attaque plus de cinq ans après leur élaboration, pour prendre le contrôle de serveurs. Dans leur immense majorité, les attaques ne remontent pas à plus de cinq ans. L'abaissement

de la durée de conservation de dix à cinq ans exclura peut-être quelques rares attaques dont l'infrastructure a été échafaudée très à l'avance, néanmoins, l'essentiel des attaques resteront dans le champ d'application du dispositif. En matière de conservation des données, la commission s'est donc arrêtée à ce compromis judicieux, dans cet article comme dans les autres. Avis défavorable.

**Mme la présidente.** La parole est à M. Antoine Léaument.

**M. Antoine Léaument.** On ne comprend plus rien ! Vous dites que dix ans de conservation des données, c'est trop. C'est pourtant le délai que prévoyait le projet de loi ; il a été réduit à cinq ans lors de l'examen en commission. Vous affirmez maintenant que la bonne durée serait cinq ans, que deux ans seraient insuffisants. Nous vous demandons pourquoi. Seul M. le ministre délégué a donné un élément de réponse, expliquant que les architectures des attaques pouvaient perdurer plus de cinq ans. Dans ce cas, il faut augmenter le délai ! Il faut le porter à cinq ans et demi, ou six, ou sept ans.

**M. Ugo Bernalicis.** C'est en effet de la sécurité nationale qu'il s'agit !

**M. Antoine Léaument.** Notre propos tend à souligner qu'on ne peut limiter les droits sans avoir de bonnes raisons. Sinon on fait n'importe quoi, comme utiliser des lois de sécurité intérieure contre des militants écologistes – ça arrive. On nous demande assez fréquemment d'adopter telle et telle mesures au nom de la lutte antiterroriste, ou de l'ordre public – M. Bernalicis a raison –, en affirmant qu'ainsi plus jamais rien de dramatique ne surviendra. Rien de grave : nous ne faisons que voter chaque année, sans encombres, une loi de sécurité, laquelle ne résout aucun problème. En revanche, les droits sont de plus en plus menacés. Maintenant, vous nous annoncez des trucs...

**M. Emeric Salmon.** Des trucs ?

**M. Antoine Léaument.** ...comme placer des mouchards dans les téléphones !

Petit à petit, on réduit les droits, encore et encore ; on applique des lois antiterroristes à d'autres desseins, sans que cela pose problème. Nous examinons ici un sujet mineur et vous êtes incapables de nous dire pourquoi deux ans, cinq ans ou dix ans seraient ou ne seraient pas des délais opportuns.

**M. Emeric Salmon.** N'importe quoi !

**M. Antoine Léaument.** Vous n'avez aucun argument rationnel. Nous ne vous demandons rien d'autre !

**M. François Piquemal.** Nous attendons.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Pourquoi dix ans ? À l'origine du débat, l'intention était de fixer un délai habituel en matière de prescription dans ce domaine, en particulier pour les délits.

Lors de l'examen du texte en commission, nous avons abouti à un compromis de cinq ans. Les auditions ont montré qu'il était inutile de conserver les données dix ans : si dans les cinq ans qui suivent une attaque, on n'a pas trouvé les personnes ou reçu de demande de coopération, il est trop tard pour identifier les auteurs. Un délai de deux ans serait trop court. La coopération internationale nous impose d'aller

au-delà. D'autres pays demandent notre soutien, dans le cadre de leurs instructions sur WannaCry, qui a eu lieu en 2017.

**M. Ugo Bernalicis.** Nous sommes en 2023, c'était donc il y a six ans ! Vous voyez bien que cinq ans, ça ne marche pas non plus !

**M. Philippe Latombe.** Certes, mais si les demandes sont déposées à l'Anssi dans les cinq ans, elle peut transmettre les données à l'autorité judiciaire, qui les gèle.

**M. Ugo Bernalicis.** Non ! le délai de cinq ans est le maximum !

**M. Philippe Latombe.** C'est pourtant ce qui s'est passé. Ce délai est donc suffisant pour que les correspondants des pays avec lesquels nous travaillons dans le domaine de la cybersécurité nous transmettent leurs demandes, et que nous soyons efficaces. (*Applaudissements sur les bancs du groupe HOR.*)

(*L'amendement n° 173 n'est pas adopté.*)

**Mme la présidente.** Sur l'article 32, je suis saisie par le groupe Démocrate (MODEM et indépendants) d'une demande de scrutin public.

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

La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n° 1273.

**M. Jérémie Iordanoff.** Il suit la même logique que l'amendement n° 170 de Mme Thomin. Lors de l'examen en commission, nous avons proposé d'instaurer une procédure de recours *ad hoc* ; Mme la rapporteure pour avis nous a opposé l'existence du référé liberté, suffisant selon elle.

Le présent amendement vise à garantir cette possibilité afin d'empêcher que soit déclaré irrecevable un recours contre les injonctions de l'Anssi formulées en application de l'article 32.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Avis défavorable, pour les mêmes raisons que celles avancées lors de l'examen de l'amendement de Mme Thomin.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Il est vrai que nous avons brièvement évoqué le juge administratif et le référé liberté lorsque nous avons proposé de porter à soixante-douze heures le délai prévu à l'alinéa 10. Vous nous avez répondu que c'était déjà satisfait en droit, qu'au pire les gens prendraient un avocat – bref, « débrouillez-vous » –, que, d'ailleurs, l'objectif n'était pas de faire valoir des droits, mais d'arrêter l'attaque et de pouvoir conserver les données afférentes pour analyser son architecture. En somme, vous avez brandi la sécurité nationale, un truc avec lequel on ne rigole pas : la saisine du juge administratif serait vraiment hors sujet.

Nous entendons tout cela, mais nous ne comprenons toujours pas pourquoi le délai devrait être de cinq ans, ou de dix, ou de deux ; de quarante-huit heures plutôt que de soixante-douze ! Vous donnez l'impression d'avoir pour seul objectif de passer le filtre du Conseil constitutionnel,...

**M. Laurent Jacobelli.** Vous, vous donnez l'impression d'avoir pour seul objectif de passer du temps en séance !

**M. Ugo Bernalicis.** ...de trouver le dispositif le plus proche de ses limites, comme s'il s'agissait d'un *crash test* permanent.

Or, dans un État de droit, on ne peut pas raisonner ainsi. Il faut des arguments logiques, rationnels et pertinents, et il faut autoriser des voies de recours, sinon on n'est plus dans le droit.

**M. Laurent Jacobelli.** Il ne faut pas rester là, monsieur !

**M. Ugo Bernalicis.** Vous citez des attaques qui se sont produites il y a plus de cinq ans, mais il n'est pas nécessaire de disposer des données exactes qui les concernent, que d'ailleurs nous n'avons plus. Lorsqu'une attaque survient, il est possible de reconstituer son architecture et de la conserver, sans stocker l'ensemble des données de l'attaquant. En cas de procédure judiciaire, les données seront conservées sous scellés le temps nécessaire à l'enquête. Le sujet n'est plus le même, le cadre non plus.

Je veux bien qu'on me raconte des carabistoules, mais voter une loi comme celle-ci, qui prévoit des moyens exorbitants du droit, sur le fondement de carabistoules...

**M. Jocelyn Dessigny, M. Laurent Jacobelli et M. Jean-Louis Thiériot.** Carabistouilles !

**M. Ugo Bernalicis.** Oui, c'est carabistouilles, mais dans le Nord, on dit carabistoules, c'est comme ça ! (*Sourires.*)

**M. Antoine Léaument.** Vous pouvez constater que M. Bernalicis ne perd pas le Nord !

**M. Ugo Bernalicis.** Donc, ça ne va pas du tout. En plus, parler de garanties devant le juge administratif... (*Mme la présidente coupe le micro de l'orateur, dont le temps de parole est écoulé.*)

**Mme la présidente.** Merci, monsieur Bernalicis. La parole est à M. Jean-Louis Thiériot.

**M. Jean-Louis Thiériot.** « Les lois inutiles affaiblissent les lois nécessaires. » Nous avons un code de justice administrative très bien fait : il prévoit les conditions de recours au référé liberté. Il est donc absurde de vouloir ajouter que cette procédure s'applique dans tel ou tel domaine.

**M. Antoine Léaument.** Vous n'aimez pas le référé liberté !

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** L'Anssi est une agence gouvernementale, qui relève directement du Premier ministre. Par son intervention, l'exécutif prend des mesures qui restreignent les libertés publiques. Au regard de l'équilibre des pouvoirs, c'est déjà discutable. Il est indispensable de prévoir au minimum une procédure de recours devant le juge administratif. Le référé liberté n'est pas automatique, il doit être recevable : le texte doit préciser quelle est la procédure. La recevabilité ne doit pas dépendre de la bonne volonté du juge, qui pourrait par exemple estimer que l'urgence n'est pas démontrée. Il faut une procédure. Nous en avons proposé une en commission et vous nous avez opposé le référé liberté : qu'est-ce qui empêche d'inscrire que la personne concernée peut saisir le juge des référés ?

(*L'amendement n° 1273 n'est pas adopté.*)

**Mme la présidente.** La parole est à M. Philippe Latombe, pour soutenir l'amendement n° 1658.

**M. Philippe Latombe.** Nous en avons discuté en commission des lois ; il vise à remplacer « surcoûts » par « coûts ». L'article 32 s'appliquera à quelque vingt attaques par an seulement, mais il s'agira d'attaques massives et coordonnées : les opérateurs devront consentir de lourds investissements pour appliquer le dispositif.

Il ne s'agit pas des retraits de contenus, auxquels on peut déjà procéder et pour lesquels on pourrait parler de surcoûts à chaque nouvelle demande. Là, les opérateurs seront obligés d'investir massivement pour effectuer des redirections vers des serveurs sécurisés – de l'Anssi par exemple – en réponse à des attaques coordonnées et massives s'appuyant sur des flux de données importants. Les mesures qu'ils devront prendre impliquent d'investir dans des logiciels de filtrage ou dans des outils dirigeant les flux de données directement sur les serveurs. Ces mesures sont bien plus complexes que celles concernant les retraits de contenus terroristes ou pédopornographiques.

Dans ce contexte, il paraît délicat d'imposer le terme de surcoûts – qui reste d'ailleurs à définir. Si les opérateurs font ces investissements, ce sera au détriment du fonctionnement normal des services qu'ils fournissent car leurs capacités d'investissement en seront obérées. Puisque nous leur demandons des mesures supplémentaires exceptionnelles impliquant des investissements importants, il est normal que les coûts en soient supportés par la collectivité, donc par l'État.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Nous en avons discuté à plusieurs reprises. J'ai interrogé à nouveau l'Anssi, qui assure que l'article 32 n'impliquera aucune dépense d'investissement pour les opérateurs concernés. Comme l'a dit M. le ministre délégué, il est question d'une dizaine d'opérations de filtrage par an. Ce nombre, qui semble raisonnable, permettra une exécution par des agents déjà embauchés, sans qu'il soit nécessaire d'appliquer un système de traitement automatisé.

La notion de coûts permet déjà de couvrir les dépenses de fonctionnement et les éventuelles dépenses inhérentes à la masse salariale mobilisée par les opérateurs. À titre personnel, compte tenu de ce qui m'a été communiqué, j'hésite entre un avis favorable et un avis défavorable...

**M. Philippe Gosselin.** Le « en même temps » !

**Mme Sabine Thillaye, rapporteure pour avis.** ...car je n'ai pas une vision très claire sur ce point. Je m'aligne donc sur l'avis défavorable de la commission.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Le dispositif prévu à l'article 32 permettra à l'Anssi d'enjoindre aux opérateurs résolveurs de DNS de créer des filtrages. La question d'un dédommagement plus élevé pourrait se poser si des investissements devaient être réalisés par ces acteurs pour l'exécution des demandes de filtrage. Or ces derniers sont déjà assujettis à de nombreuses demandes de filtrage, issues de demandes administratives – je l'ai dit tout à l'heure.

Il convient donc de s'assurer que les dépenses de fonctionnement supplémentaires sont bien dédommagées – c'est l'objectif de l'amendement. Il ne s'agit pas d'imposer aux

acteurs des opérations sans les en dédommager. C'est pourquoi l'article dispose que les surcoûts, c'est-à-dire les dépenses de fonctionnement supplémentaires, doivent être compensés par l'État. Votre proposition, qui vise à aller plus loin en englobant les coûts, nous paraît donc excessive : son adoption engendrerait des charges considérables pour les finances publiques, qui iraient au-delà de celles résultant de ces nouvelles mesures, qui concerneront un nombre limité de cas. Demande de retrait ou avis défavorable.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** L'alinéa 15 de l'article 32 prévoit donc de dédommager des opérateurs qui auraient l'obligation de respecter la loi. Voilà un concept intéressant : dédommager des gens parce qu'ils devront respecter la loi. J'ignore s'il existe des cas de figure équivalents : les réquisitions peuvent être, mais il ne s'agit pas ici de réquisitions. Nous aurions sans doute moins de difficultés si on renationalisait le secteur des télécommunications, mais c'est un autre sujet.

**M. Antoine Léaument.** Très bonne idée !

**M. Jocelyn Dessigny.** Merci, au revoir !

**M. Ugo Bernalicis.** Le collègue Latombe pousse la logique jusqu'à son terme : la sécurité nationale demande peut-être la création de machins et de gros filtres pour arrêter les assaillants, mais les opérateurs n'ont pas que ça à faire ! En plus, développer des machins pour le compte de l'État, pour protéger la sécurité nationale, ça leur coûte des sous alors qu'ils cherchent à en gagner !

**M. Jocelyn Dessigny.** Des trucs, des machins, un vrai vocabulaire !

**M. Jean-Louis Thiériot.** Et des bidules aussi !

**M. Ugo Bernalicis.** Mon cœur balance : soit on va au bout de la logique et on considère que c'est à l'argent public d'assumer des mesures d'intérêt public, plutôt qu'aux fournisseurs d'accès ; soit on considère que la sécurité est l'affaire de tous – c'est un slogan à vous, non ? Dans le cadre du fameux continuum de sécurité, les opérateurs pourraient s'assurer, y compris financièrement, que leurs – nos – systèmes ne sont pas utilisés à des fins malveillantes.

Pour ces raisons, je suis défavorable à l'amendement de M. Latombe. Les opérateurs peuvent mettre un peu la main à la poche ; en réalité, ils peuvent même la mettre entièrement, parce que c'est aussi dans leur intérêt.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Votre argument, monsieur le ministre délégué, selon lequel il ne s'agit que d'une couche supplémentaire de dépenses, est en contradiction avec les propos tenus par les représentants des opérateurs que nous avons auditionnés. Cela illustre la divergence entre le travail parlementaire et les propositions faites par vos services. Les opérateurs nous ont expliqué qu'ils devront faire des investissements très importants pour répondre aux obligations prévues dans le texte : même si les cas de figure sont limités, les flux de données seront massifs et devront être redirigés vers des serveurs sécurisés de l'Anssi ou faire l'objet d'un filtrage. Cela nécessite des investissements qui se feront forcément au détriment d'investissements dans les réseaux et destinés à la collectivité, c'est-à-dire à l'ensemble de nos concitoyens.

**M. Ugo Bernalicis.** Le business !

**M. Philippe Latombe.** Par ailleurs, pour répondre à M. Bernalicis, remplacer le terme de coûts par celui de surcoûts limitera peut-être le nombre de demandes de redirections de DNS et de filtres de la part de l'Anssi; ce serait, éventuellement, une mesure de contrôle.

**M. Ugo Bernalicis.** Mais il ne faut pas ! Il est question de la sécurité nationale, enfin, camarade !

**Mme la présidente.** La parole est à M. le ministre délégué.

**M. Jean-Noël Barrot, ministre délégué.** J'imagine bien que les acteurs concernés par l'article 32 ont signalé à la représentation nationale les coûts très considérables qu'engendrerait pour eux l'application de ces mesures de filtrage. Dans la loi pour la confiance dans l'économie numérique, dite LCEN, les capacités données à la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) pour opérer un filtrage prévoient une compensation des surcoûts de fonctionnement.

**M. Ugo Bernalicis.** C'est déjà sympa, en fait !

**M. Jean-Noël Barrot, ministre délégué.** Cette capacité a notamment été appliquée lors du déréférencement de la plateforme de commerce Wish – ce n'était pas exactement une mesure de filtrage.

**M. Philippe Latombe.** C'était un déréférencement.

*(L'amendement n° 1658 n'est pas adopté.)*

**Mme la présidente.** Je mets aux voix l'article 32, tel qu'il a été amendé.

*(Il est procédé au scrutin.)*

**Mme la présidente.** Voici le résultat du scrutin :

Nombre de votants .....	62
Nombre de suffrages exprimés .....	58
Majorité absolue .....	30
Pour l'adoption .....	51
contre .....	7

*(L'article 32, amendé, est adopté.)*

### Article 33

**Mme la présidente.** La parole est à Mme Clara Chassaniol, première inscrite sur l'article 33.

**Mme Clara Chassaniol.** L'article 33 prévoit la communication à l'Anssi de certaines données de cache des serveurs de DNS. Pour que chacun comprenne bien ce qui est visé, rappelons que les résolveurs DNS sont les machines qui font le lien entre un nom de domaine et l'adresse IP – *internet protocol* – d'un utilisateur qui souhaite y accéder. Afin de répondre rapidement à l'utilisateur, ces serveurs conservent des données qui sont dites de cache. Or celles-ci ne peuvent être transmises à l'Anssi, alors qu'elles éclaireraient sur les infrastructures informatiques utilisées par les cyberattaquants. L'Anssi aurait ainsi accès aux causes des cyberattaques et non seulement à leurs effets.

Cet article prévoit l'obtention de la copie des données de cache des serveurs DNS : les noms de domaine, les adresses IP des machines utilisées et l'horodatage des demandes. Il sera ainsi possible de connaître avec précision les modes opéra-

toires des cyberattaquants. Ces données sont stratégiques pour perfectionner nos dispositifs de détection des menaces et de contre-attaque. Le dispositif prévu à l'article 33 fait évidemment l'objet d'un contrôle de l'Arcep, qui figure à l'article 35.

L'article 33 prévoit d'autres garanties essentielles, en excluant les données identifiantes de la copie autorisée par l'Anssi – nous en avons longuement parlé en commission. Je défendrai d'ailleurs un amendement visant à instaurer l'anonymisation des données qui peuvent être recueillies par l'Anssi.

Cet article défend la stratégie de cyberdéfense ; il vise à adapter nos connaissances et nos réactions à l'évolution des menaces, tout en préservant l'équilibre fondamental, qui nous est cher, entre la nécessité de se défendre et nos droits et libertés.

**Mme la présidente.** La parole est à Mme Anne Le Hénanff.

**Mme Anne Le Hénanff.** L'article 33 permet aux agents de l'Anssi d'être destinataires des données techniques non identifiantes enregistrées temporairement sur les serveurs des opérateurs de communication électronique et des fournisseurs de systèmes de résolution de nom de domaine, à des fins de détection et de caractérisation des attaques informatiques.

Le groupe Horizons et apparentés est favorable à cet article, auquel plusieurs précisions ont été apportées en commission : sur le cadre des pouvoirs conférés à l'Anssi, sur les délais de conservation des données ou encore sur les avis des autorités indépendantes. La suppression des opérateurs de communication électronique du champ de cet article nous semble également être une bonne chose.

Enfin, il nous a paru nécessaire de préciser que les adresses IP sources ne peuvent être ni recueillies ni exploitées. C'est pourquoi le groupe Horizons et apparentés a déposé un amendement fondamental, qui a été retravaillé à l'issue des travaux en commission : il vise à préciser que les données transmises aux agents de l'Anssi doivent être anonymisées par les fournisseurs de systèmes de résolution de noms de domaine. Nous espérons également que les débats permettront de préciser quelles sont les catégories de données identifiantes.

**Mme la présidente.** La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n° 1270.

**M. Jérémie Iordanoff.** Veuillez m'excuser d'insister sur la notion de sécurité nationale ; j'y reviendrai encore lors de l'examen des deux articles suivants. Cet amendement vise à la remplacer par la notion d'intérêts fondamentaux de la nation, qui a le mérite d'être précise et dont les éléments sont énumérés quelque part.

Vous avez dit dans cet hémicycle qu'il ne fallait pas renvoyer au code pénal ; en commission, vous avez dit qu'il ne fallait pas renvoyer au code de sécurité intérieure. J'entends bien qu'il ne faut renvoyer à rien, mais il faut tout de même définir ce qu'est la notion de sécurité nationale !

Tout à l'heure, vous avez évoqué une décision du Conseil constitutionnel : pouvez-vous préciser laquelle et indiquer comment ce dernier caractérise exactement la sécurité nationale ? Je n'ai pas trouvé de définition satisfaisante. Le législateur devrait préciser cette notion et ne pas la laisser à la jurisprudence, à moins qu'on ait une définition précise ; en ce cas, je vous laisse nous dire de quoi il retourne exactement.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Même avis – défavorable – que sur l'amendement n° 1269 ; nous nous sommes déjà exprimés à ce sujet. En commission, nous avons fait évoluer les dispositifs parce qu'il n'y avait aucune référence à la défense de la sécurité nationale dans le texte, en dehors de l'article 32. Nous avons rattaché tous les articles à cette notion, ce qui me semble apporter des garanties beaucoup plus larges.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis que la rapporteure et même avis que sur les amendements semblables, à l'article 32. Dans le cadre de l'examen d'une QPC posée par des opérateurs de télécommunication électronique contre la loi « 5G », le Conseil constitutionnel a jugé que la sécurité nationale avait été définie de façon suffisamment précise par le législateur.

**M. Jérémie Iordanoff.** Dans quel texte ?

**M. Jean-Noël Barrot, ministre délégué.** Je me réfère à la décision n° 2020-882 du 5 février 2021.

**Mme la présidente.** La parole est à Mme Anne Le Héanff.

**Mme Anne Le Héanff.** Il semble nécessaire de rappeler régulièrement que le chapitre V fait bien partie de la loi de programmation militaire.

**M. Mounir Belhamiti.** Merci de le rappeler !

**Mme Anne Le Héanff.** En effet, certaines interventions dérivent vers des sujets qui n'en relèvent pas. (*Applaudissements sur les bancs du groupe HOR et sur quelques bancs des groupes Dem et RE.*)

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** J'ai bien lu la décision en question : elle évoque la sécurité nationale sans la définir.

**M. Ugo Bernalicis.** Eh oui !

**M. Jérémie Iordanoff.** Les seuls éléments mentionnés qui s'y rapportent sont les « règles relatives à la permanence, à l'intégrité, à la sécurité ou à la disponibilité du réseau ou relatives à la confidentialité des messages transmis et des informations liées aux communications ». Soit ces précisions sont trop restrictives et le contrôle du respect de ces règles ne relèvera pas des prérogatives de l'Anssi, soit elles sont hors sujet. Quoi qu'il en soit, pourquoi le législateur ne pourrait-il pas définir cette notion ?

**M. Ugo Bernalicis.** Il a raison !

**M. Jérémie Iordanoff.** Les juges européens rencontreront des difficultés en raison de cette imprécision – j'y reviendrai tout à l'heure.

(*L'amendement n° 1270 n'est pas adopté.*)

**Mme la présidente.** L'amendement n° 775 de Mme la rapporteure pour avis est rédactionnel.

(*L'amendement n° 775, accepté par le Gouvernement, est adopté.*)

**Mme la présidente.** L'amendement n° 1275 de M. Jérémie Iordanoff est défendu.

(*L'amendement n° 1275, repoussé par la commission et le Gouvernement, n'est pas adopté.*)

**Mme la présidente.** La parole est à M. Philippe Latombe, pour soutenir les amendements n° 1587 et 1618, qui peuvent faire l'objet d'une présentation groupée.

**M. Philippe Latombe.** Je retire les amendements n° 1587 et 1618 au bénéfice des amendements identiques n° 1626 et 1669. Nous avons discuté de cette question en commission des lois et sommes convenus que Mmes Chassaniol et Le Héanff réécriraient leurs amendements en vue de la séance, ce qui a été fait. Mes amendements n'ont donc plus de raison d'être.

(*Les amendements n° 1587 et 1618 sont retirés.*)

**Mme la présidente.** Je suis saisie de deux amendements identiques, n° 1626 et 1669, qui font l'objet d'un sous-amendement n° 1791.

La parole est à Mme Clara Chassaniol, pour soutenir l'amendement n° 1626.

**Mme Clara Chassaniol.** Il vise à préciser que les données transmises à l'Anssi doivent être anonymisées par les fournisseurs de système de résolution de noms de domaine, sans mentionner l'adresse IP source, afin de préserver l'anonymat de l'utilisateur du nom de domaine et de cibler seulement les données qui permettraient de reconstituer un type d'attaque. Il s'agit donc de sécuriser l'anonymat des données recueillies par l'Anssi.

J'en profite pour remercier la rapporteure pour avis, le Gouvernement et l'Anssi pour leur collaboration entre la commission et la séance. À l'issue de ces discussions, il est apparu que l'inscription d'une liste de données techniques ne garantirait pas réellement l'anonymat de ces données car elles peuvent évoluer et devenir identifiantes.

**Mme la présidente.** La parole est à Mme Anne Le Héanff, pour soutenir l'amendement identique n° 1669.

**Mme Anne Le Héanff.** Il vise à préciser que les données transmises aux agents de l'Anssi doivent être anonymisées par les fournisseurs de système de résolution de noms de domaine. En effet, ces données ne doivent en aucun cas permettre une identification, ce qui est explicitement écrit dans l'étude d'impact du présent projet de loi. Ces amendements complètent l'amendement n° DN952 de Mme la rapporteure, adopté en commission des lois, qui précise que « les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés ne peuvent être ni recueillies ni exploitées. »

**Mme la présidente.** Le sous-amendement n° 1791 de Mme la rapporteure pour avis est rédactionnel.

Quel est l'avis de la commission sur les amendements identiques ?

**Mme Sabine Thillaye, rapporteure pour avis.** J'émet un avis favorable car ils visent à préciser utilement le dispositif. Nous avons adopté un amendement qui prévoit la consultation de la Cnil avant la publication du décret en Conseil d'État précisant les modalités d'application de l'article 33.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Je suis également favorable à ces amendements identiques ainsi sous-amendés par Mme la rapporteure pour avis. Je saisis l'occasion, ainsi que je l'avais fait lors de l'examen de l'article 32, pour saluer les travaux en commission, qui ont permis d'affiner et de resserrer le dispositif. En effet, vous avez adopté un amendement qui fait référence à la sécurité nationale; un amendement qui prévoit la consultation de la Cnil avant la publication du décret en Conseil d'État; un amendement qui vise à encadrer la durée de conservation des données non identifiantes, qui passe de dix à cinq ans; enfin, un amendement de la rapporteure pour avis, qui vise à préciser que les données « permettant d'identifier la source de la connexion et celles relatives aux équipements terminaux utilisés ne peuvent être ni recueillies ni exploitées », garantissant un premier niveau de sécurité. Ces amendements viennent utilement compléter ce dispositif.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** En commission des lois, nous avons indiqué que l'article 33 devait être sérieusement retravaillé afin qu'il soit beaucoup plus sécurisé. C'est pourquoi je soutiens ces amendements, ainsi que le sous-amendement. En effet, ils viennent compléter une série d'amendements adoptés en commission des lois. L'un d'eux fait référence à la sécurité nationale, notion dont nous avons débattu tout à l'heure. À cette occasion, nous avons rappelé la décision du Conseil constitutionnel qui la définit très clairement.

Ces amendements sont en outre de nature à rendre plus claire la rédaction du décret à contraindre l'autorité administrative à fixer la durée de conservation des données non identifiantes. Voilà qui facilitera la validation du projet de décret par la Cnil. Le fait, en effet, de préciser que les données collectées seront rendues anonymes permettra à la Cnil – qui en indiquera les modalités – d'effectuer un contrôle *a priori* puis un contrôle *a posteriori* nécessaires en vue d'apporter des garanties à nos concitoyens.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** J'ai salué l'initiative de la collègue Chassaniol et nous voterons ces amendements. J'aimerais que l'on se souvienne de l'étude d'impact, qui indique que les données recueillies ne seront ni identifiantes ni personnelles. Or, lorsqu'on a une connaissance de ces données techniques, on sait que, assez facilement, on peut réussir à identifier les personnes derrière les adresses IP et Mac, les données identifiantes de chaque appareil étant uniques au monde, et à connaître leur LAN – *local area network*, réseau local – ainsi que leur position géographique approximative. Grâce à ces données, on peut apprendre beaucoup de choses – c'est d'ailleurs assez génial.

**M. Antoine Léaument.** Il a raison !

**M. Ugo Bernalicis.** Du reste, grâce à la collecte de données en cache, on réalise des campagnes de publicités qui ciblent plus spécifiquement certaines personnes – je ne m'étendrai pas davantage sur ce sujet. Pour conclure, je me réjouis qu'au bout du compte on ne croie pas sur parole l'étude d'impact du Gouvernement.

**M. Jean-Noël Barrot, ministre délégué.** Cela s'appelle la démocratie parlementaire.

*(Le sous-amendement n° 1791 est adopté.)*

*(Les amendements identiques n° 1626 et 1669, sous-amendés, sont adoptés.)*

**Mme la présidente.** Sur l'article 33, je suis saisie par le groupe Démocrate (MODEM et indépendants) d'une demande de scrutin public.

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

La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n° 174.

**Mme Mélanie Thomin.** Il est en lien avec celui défendu à l'article 32. Nous nous interrogeons sur les délais proposés pour la conservation des données. Le choix de la durée de cinq ans nous paraît, encore une fois, arbitraire et les arguments avancés tout à l'heure ne parviennent pas à nous convaincre. Nous considérons qu'il ne s'agit pas de répondre aux contraintes de fonctionnement de l'administration, ce qui témoigne de peu de volonté politique, mais qu'il revient à l'administration de se conformer aux délais prescrits. Dès lors, donnons à l'Anssi les moyens d'agir avec efficacité.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Nous n'aurons jamais de réponses claires sur la question des délais. Tout à l'heure, M. le ministre délégué a dit que la durée de cinq ans n'était pas suffisante, tandis que M. Latombe a évoqué un cas datant de 2017, ce qui fait six ans, si mes calculs sont bons – si, comme je le crois, nous sommes bien en 2023. Êtes-vous bien certain qu'un délai de cinq ans serait suffisant, monsieur le ministre délégué ?

**M. Jean-Noël Barrot, ministre délégué.** Oui !

**M. Ugo Bernalicis.** Si ces données sont certes non identifiantes, elles peuvent se révéler importantes, du point de vue de la sécurité nationale, pour retracer une attaque. La durée de deux ans est raisonnable. On doit pouvoir reconstituer sur papier l'architecture de l'attaque qui serait lancée, il est nul besoin de disposer de données à chaque étape, d'autant qu'elles ne sont pas identifiantes. Dès lors, je ne vois aucune raison de les conserver aussi longtemps.

Une fois de plus, ces dispositions sont nébuleuses et donnent l'impression qu'elles ont été rédigées sur un coin de table. C'est un peu dommage car ces dispositions sont utiles – du reste, je suis plutôt favorable à l'article 33. Si la durée de conservation des données était de deux ans, ce serait parfait; nous serions presque d'accord à 100 % avec vous, monsieur le ministre délégué.

*(L'amendement n° 174 n'est pas adopté.)*

**Mme la présidente.** La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n° 1272.

**M. Jérémie Iordanoff.** C'est un amendement de repli par rapport à l'amendement n° 1275 que j'ai défendu sans prendre le temps de le présenter. Celui-ci visait à limiter l'obligation de transmission des données au seul cas où elle serait demandée par l'Anssi, étant donné que leur volume est très important et que les données de tous seront transmises,

même si aucune attaque n'est commise. Nous avons débattu de cet amendement en commission, donc je connais votre avis sur cette question.

L'amendement n° 1272 vise à préciser par décret la fréquence et les conditions de transmission des données, transmission qui fait peser une charge sur les acteurs concernés. Il ressort des auditions menées que cette transmission doit être précisée par décret.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure.** Cette précision est utile. Avis favorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Il ne faut pas surestimer le volume des données traitées, puisque l'Anssi n'analyse que la correspondance entre les noms de domaine et les adresses IP, une fois anonymisées, c'est-à-dire une fois l'adresse IP source extraite.

**M. Maxime Minot.** C'est déjà beaucoup !

**M. Jean-Noël Barrot, ministre délégué.** Toutefois, le présent amendement est utile afin de faciliter la rédaction du décret. J'émet également un avis favorable sur cet amendement.

*(L'amendement n° 1272 est adopté.)*

**Mme la présidente.** Je mets aux voix l'article 33.

*(Il est procédé au scrutin.)*

**Mme la présidente.** Voici le résultat du scrutin :

Nombre de votants .....	58
Nombre de suffrages exprimés .....	55
Majorité absolue .....	28
Pour l'adoption .....	55
contre .....	0

*(L'article 33, amendé, est adopté.)*

### Article 34

**Mme la présidente.** La parole est à Mme Anne Le Hénanff, inscrite sur l'article 34.

**Mme Anne Le Hénanff.** Cet article renforce les exigences de transparence qui s'appliquent aux éditeurs de logiciels, en contraignant ces derniers à informer l'Anssi et leurs utilisateurs en cas de vulnérabilité significative ou d'incident informatique susceptibles d'affecter un de leurs produits.

Le groupe Horizons et apparentés a déposé plusieurs amendements en commission et en séance afin d'apporter des précisions ou d'en demander. Ainsi, nous avons déposé un amendement, retravaillé à l'issue de l'examen du texte en commission, visant à définir l'éditeur de logiciels de manière claire dans le projet de loi. Nous avons également déposé en séance un amendement visant à ce que le type de vulnérabilité et d'incident informatique devant faire l'objet d'un signalement à l'Anssi soit précisé par décret. Aussi sommes-nous satisfaits par l'amendement présenté par Mme la rapporteure qui va dans ce sens.

Notre groupe se réjouit également de l'adoption en commission d'amendements de clarification, relatifs tant aux exigences de transparence qu'aux délais auxquels sont soumis les éditeurs de logiciels pour informer l'Anssi des failles et incidents, et définissant certaines notions dans la loi. Ces amendements visent réellement à préciser le cadre dans lequel s'inscrit cet article et nous espérons que nous aborderons, avec le même esprit, l'examen des amendements.

**Mme la présidente.** La parole est à M. Philippe Latombe, pour soutenir l'amendement n° 1664.

**M. Philippe Latombe.** Il s'agit d'un amendement de cohérence puisqu'il vise à introduire à l'article 34 la référence à la sécurité nationale qui figure dans les articles 32, 33 et 35.

Pour revenir au débat suscité par les amendements de M. Iordanoff, je précise que le Conseil constitutionnel vise, dans sa décision du 5 février 2021 citée tout à l'heure, les « installations dont l'indisponibilité risquerait de diminuer d'une façon importante – et il en vient ici à la définition de la sécurité nationale – le potentiel de guerre de la nation, son potentiel économique, sa sécurité ou sa capacité de survie et qui, de ce fait, sont tenues de coopérer à la protection de ces installations contre toute menace ».

Cette définition est donc suffisamment large pour englober les cas d'attaques cyber tout en étant très précise, davantage en tout cas que celle du code pénal que vous proposiez de retenir, monsieur Iordanoff. Il n'est pas question ici des installations culturelles, par exemple.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Nous partageons l'objectif visé mais, aux termes de l'article 34, il est de la responsabilité des éditeurs de logiciels de déclarer leurs vulnérabilités. Or ceux-ci ne sont pas habilités à apprécier l'atteinte à la sécurité nationale, qui est une prérogative de l'État. En commission, nous avons néanmoins souhaité mieux définir ce qu'est un incident informatique et préciser le caractère significatif des incidents et vulnérabilités visés, par trois amendements que nous allons examiner dans quelques instants.

Par ailleurs, j'émettrai un avis favorable à votre amendement n° 1673, qui prévoit que le délai fixé par l'Anssi pour informer les utilisateurs professionnels « est déterminé en fonction de l'urgence, des risques pour la sécurité nationale et du temps nécessaire aux éditeurs pour prendre les mesures correctives ».

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Il est utile de préciser dans cet article, comme c'est le cas aux articles 32 et 33, que c'est bien la sécurité nationale qui est en jeu. Du reste, je remercie Mme Le Hénanff d'avoir rappelé que nos travaux s'inscrivent dans le cadre de l'examen d'un projet de loi de programmation militaire.

Toutefois, à l'instar de Mme la rapporteure pour avis, je propose que vous retiriez cet amendement au profit du n° 1673 car il nous semble que c'est à l'Anssi d'estimer ce qui relève ou non de la sécurité nationale, que les éditeurs de logiciels n'ont peut-être pas tout à fait la capacité d'apprécier.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Je retire l'amendement au profit du n° 1673. Ce qui importe, c'est qu'il soit fait référence à la sécurité nationale puisque, en effet, nous examinons un projet de loi de programmation militaire et que nous modifions le code de la défense.

*(L'amendement n° 1664 est retiré.)*

**Mme la présidente.** Sur l'amendement n° 176, je suis saisie par le groupe Socialistes et apparentés (membre de l'intergroupe NUPES) d'une demande de scrutin public.

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

Je suis saisie de trois amendements, n° 838, 994 et 176, pouvant être soumis à une discussion commune.

Les amendements n° 838 et 994 sont identiques.

L'amendement n° 838 de M. Aurélien Saintoul est défendu.

La parole est à M. Ugo Bernalicis, pour soutenir l'amendement n° 994.

**M. Ugo Bernalicis.** Si les éditeurs de logiciels libres, pardon : de logiciels – libres ou pas : peu importe – ont l'obligation de transmettre à l'Anssi les failles de sécurité qui affectent leurs produits ou les incidents qui peuvent compromettre la sécurité nationale, il serait bon qu'ils puissent être sanctionnés s'ils ne le font pas. Il est en effet probable qu'ils n'auront pas tous envie de coopérer de manière immédiate et qu'ils chercheront à gagner du temps, dans la mesure où le fait de révéler les failles de sécurité d'un de vos logiciels peut nuire à votre réputation d'éditeur et inciter les administrations à ne pas l'utiliser, par exemple.

Ainsi, les éditeurs pourraient avoir la tentation capitalistique – c'est une hypothèse – de ne pas dévoiler les failles dans les délais exigés, si bien que la France serait dans la panade du point de vue de la défense de ses intérêts vitaux.

En outre, puisque nos administrations utilisent beaucoup de solutions logicielles privées sur lesquelles elles n'ont pas trop la main et qu'elles ont été attaquées – je pense au ministère de la justice, il y a environ un an, ou à l'Assemblée nationale, récemment –, on n'a pas trop envie de rigoler avec un éditeur de logiciels qui ne coopérerait pas spontanément et immédiatement.

Il nous semble donc intéressant de suspendre au-dessus de leur tête une petite épée de Damoclès, en l'espèce une amende pouvant aller jusqu'à 4 % de leur chiffre d'affaires. Nos camarades socialistes proposeront 1 %. Peu importe : dès lors que le principe d'une sanction est retenu, le dispositif sera plus utile, y compris à l'Anssi, dans son rapport de force avec les éditeurs de logiciels.

**Mme la présidente.** La parole est à M. Antoine Léaument.

**M. Antoine Léaument.** La question qui se pose ici est celle de savoir si les éditeurs de logiciels transmettront les informations relatives aux vulnérabilités que présentent leurs propres produits, sachant, comme vient de l'expliquer notre collègue Bernalicis, que le public risque alors de se montrer peu enclin à les utiliser.

Par conséquent, si l'on ne prévoit aucune sanction pour non-respect de l'obligation de signaler les failles de sécurité, le plus vraisemblable est que ces dernières ne seront pas rendues publiques ni communiquées à l'Anssi. Aussi proposons-nous, par ces amendements, que les éditeurs qui ne rempliraient pas leur obligation en la matière soient passibles d'une sanction financière. Il ne s'agit pas, pour le coup, de punir les entreprises ou je ne sais quoi : il y va de la sécurité nationale.

Par ailleurs – j'aborde là une question plus large –, on peut se demander si certains éditeurs de logiciels ne sont pas un danger pour la sécurité nationale. Je pense, par exemple, à Microsoft.

**M. Ugo Bernalicis.** Ah !

**M. Antoine Léaument.** N'oublions pas que Snowden a révélé que certaines entreprises participaient à l'espionnage.

**M. Ugo Bernalicis.** Ah bon ?

**M. Erwan Balanat.** On pourrait parler aussi d'Apple !

**M. Antoine Léaument.** Ou de TikTok, entre autres : je suis d'accord. Si l'on va au bout de ce raisonnement, on peut estimer qu'il serait intéressant d'utiliser des logiciels libres, qui non seulement sont plus sécurisés mais échappent aux logiques capitalistiques, de sorte que leurs concepteurs n'auraient pas de difficultés à déclarer leurs failles de sécurité.

**Mme la présidente.** La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n° 176.

**Mme Mélanie Thomin.** Cet amendement de bon sens vise à rendre obligatoire la communication à l'Anssi de tout incident informatique au sein d'une entreprise. En effet, on peut considérer qu'en l'absence de sanction, le monde de l'entreprise aura tendance à ne pas respecter l'obligation. Nous proposons donc que l'Anssi puisse sanctionner son non-respect en infligeant à l'entreprise concernée une pénalité d'un montant limité à 1 % du chiffre d'affaires, ce qui est tout à fait raisonnable – nos collègues du groupe LFI proposent un montant plus élevé. Quoi qu'il en soit, le dispositif ainsi consolidé inciterait davantage les entreprises à jouer le jeu.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Je tiens à souligner que nous nous efforçons, depuis le début de notre discussion, de maintenir un équilibre entre, d'une part, la sécurité nationale et, d'autre part, nos libertés fondamentales, notamment la liberté d'agir et d'entreprendre, qui nous incite à limiter les contraintes pesant sur nos entreprises. En l'espèce, je souhaite que nous nous en tenions au dispositif prévu dans le texte, à savoir qu'en cas de non-respect de l'injonction de communiquer les vulnérabilités constatées à l'Anssi, celle-ci pratiquera le fameux *name and shame*.

Au demeurant, aucune entreprise n'a intérêt à les dissimuler : son intérêt commercial est que le produit qu'elle vend fonctionne. Cela étant, le dispositif est au début de son existence : rien ne nous empêche de le faire évoluer par la suite si l'on considère qu'il est insuffisant. En tout état de cause, j'estime, pour l'instant, que nous devons limiter les contraintes qui pèsent sur les personnes et les structures concernées. Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Je suis de l'avis de la rapporteure pour avis : l'article 34 enrichi par les travaux en commission permettra d'atteindre l'objectif poursuivi. Je ne crois pas que les sanctions proposées renforceraient le dispositif, et ce pour deux raisons.

Premièrement, compte tenu du pouvoir conféré à l'Anssi de diffuser l'information concernant la vulnérabilité d'un logiciel, l'entreprise s'exposerait à une sanction réputationnelle très lourde.

**M. Antoine Léaument.** C'est l'inverse !

**M. Jean-Noël Barrot, ministre délégué.** Si l'Anssi détecte une vulnérabilité dont elle n'aurait pas été préalablement informée par l'éditeur du logiciel, elle pourra publier et faire connaître cette vulnérabilité.

**M. Ugo Bernalicis.** « Pourra » !

**M. Jean-Noël Barrot, ministre délégué.** C'est une sanction réputationnelle très lourde. En l'état actuel des choses, en l'absence de fondement législatif, l'Anssi s'exposerait à un contentieux si elle s'autorisait à publier ces vulnérabilités. C'est la raison pour laquelle elle est très réticente à le faire. L'article 34 le lui permettra.

Faut-il donner à cette agence des pouvoirs de sanction administrative ? C'est un peu compliqué dans la mesure où, vous l'avez rappelé environ soixante-dix fois depuis le début de notre débat, elle n'est pas une autorité administrative indépendante.

**M. Ugo Bernalicis.** Et alors ?

**M. Jean-Noël Barrot, ministre délégué.** Elle n'a pas de collège de sanction.

**M. Ugo Bernalicis.** Il y a beaucoup de structures étatiques qui prononcent des sanctions sans être des autorités administratives indépendantes !

**M. Jean-Noël Barrot, ministre délégué.** Elle n'est donc pas entourée de suffisamment de précautions pour prononcer de telles sanctions. L'équilibre trouvé durant les travaux en commission est le bon. Avis défavorable, donc.

**M. Ugo Bernalicis.** La DGCCRF n'est pas une autorité administrative indépendante et elle inflige des sanctions à tour de bras !

**Mme la présidente.** La parole est à M. Mounir Belhamiti.

**M. Mounir Belhamiti.** En matière de communication des anomalies logicielles, des failles informatiques, il existe deux approches.

La première, dogmatique, vient d'être défendue du côté gauche de l'Hémicycle.

**M. Antoine Léaument.** Oh !

**M. Mounir Belhamiti.** Les tenants de cette approche considèrent qu'il faut adopter une posture anticapitaliste vis-à-vis des éditeurs de logiciels. Elle est dogmatique, et M. Bernalicis l'a démontré lorsqu'il a évoqué, dans un lapsus, les logiciels libres. De très nombreuses failles logicielles, y compris celles qui sont intégrées dans des logiciels d'éditeurs capitalistes, si je puis dire, proviennent en fait de développements de la communauté du logiciel libre. Or on ne peut pas sanctionner, comme vous le proposez, une communauté de développeurs de logiciels libres.

La seconde approche, pragmatique, défendue par le ministre délégué, consiste à considérer que les éditeurs de logiciels ont tout intérêt, pour conserver et développer leur clientèle, à communiquer rapidement les failles et anomalies logicielles afin qu'elles soient corrigées et que leurs clients soient assurés de la sécurité de leur système d'information.

Pour ces différentes raisons, nous nous opposerons à l'approche de nos collègues de La France insoumise.

**Mme la présidente.** La parole est à M. Antoine Léaument.

**M. Antoine Léaument.** Eh bien, nous voilà dans le vif du sujet ! Ce n'est pas dogmatique de défendre la sécurité nationale, c'est patriote, et quand nous disons que le capitalisme peut être un problème pour la sécurité nationale, c'est pas sur la base d'un dogme mais de faits avérés. Je vous ai rappelé que des entreprises capitalistiques mues par des logiques de rentabilité avaient déjà posé des problèmes à la sécurité nationale, et nous pouvons d'ailleurs remercier chaleureusement MM. Assange et Snowden qui, pour avoir révélé un certain nombre de ces problèmes, ont ensuite subi des attaques d'une extrême violence.

Vous me reprochez de proposer des sanctions financières tout en plaidant pour le logiciel libre. Ce que j'ai dit c'est que, dans une logique capitaliste, il faut des sanctions financières car les dirigeants de firme ne comprennent que ça : ils ont un portefeuille à la place du cœur, et seules les sanctions financières les pousseront à agir.

Quant à votre argument, monsieur le ministre délégué, qui consiste à dire que les failles doivent être déclarées à l'Anssi pour éviter qu'elles soient rendues publiques, il est catastrophique ! Mieux vaut infliger des sanctions aux entreprises pour les obliger à révéler les failles, quitte, ensuite, à voir si elles sont rendues publiques ou non – c'est l'Anssi qui décidera.

Pour conclure, sur le logiciel libre, l'idée est que, puisque l'on sort des logiques capitalistes, il n'y a plus besoin de prévoir de sanctions, pour la bonne et simple raison qu'un concepteur de logiciel libre a tout intérêt à en dévoiler les failles car la communauté va s'en emparer pour les résoudre. C'est pourquoi le logiciel libre est, d'une manière générale, à la fois plus sûr, moins cher et pose moins de problèmes que ceux que l'on peut redouter avec Microsoft.

**M. Mounir Belhamiti.** C'est faux ! Ça ne marche pas du tout.

**M. Ugo Bernalicis.** D'ailleurs, dans Microsoft, il y a « micro », c'est un indice...

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** Madame la rapporteure pour avis, vous prétendez vouloir trouver une solution équilibrée entre la sécurité et les libertés individuelles, mais nous regrettons que, lorsque nous faisons des propositions en ce sens, vous ne vous préoccupez pas de cet équilibre, qu'il s'agisse de la définition du périmètre ou des voies de recours, mais seulement de ne pas nuire aux entreprises.

En réalité, ce n'est pas le sujet. La question est que l'on crée une obligation, mais sans sanction, ce qui revient à annuler cette obligation. Pour l'entreprise, ce n'est pas une question de bonne volonté, c'est une question d'intérêts économiques : elle n'a pas intérêt à rendre ses failles publiques. Vous expli-

quez que l'Anssi pourra le faire, mais il faudrait au minimum que ce soit automatique et qu'il y ait des sanctions. Le groupe Écologiste soutiendra donc ces amendements.

**Mme la présidente.** La parole est à Mme Mélanie Thomin.

**Mme Mélanie Thomin.** Madame la rapporteure pour avis, à vous entendre, l'intérêt commercial des entreprises primerait sur la sécurité nationale.

**Mme Sabine Thillaye, rapporteure pour avis.** Je n'ai pas dit ça !

**Mme Mélanie Thomin.** C'est d'autant plus grave que nous sommes en train de débattre d'une loi de programmation militaire. (*MM. Ugo Bernalicis et Antoine Léaument applaudissent.*) Notre réflexion se doit d'être à la hauteur des enjeux. Posons-nous les bonnes questions : les intérêts économiques priment-ils sur les intérêts de notre défense ? Il me semble indispensable de bien faire le distinguo, et vos propos entretiennent une certaine confusion.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Je comprends la logique de ces amendements, qui soulèvent plusieurs questions, notamment celle de l'imbrication entre les logiciels libres et ceux des éditeurs commerciaux. Se pose aussi la question de la vitesse de divulgation des failles, dans la mesure où, si on ne dispose pas des correctifs, cette divulgation devient problématique, d'autant que je vous entends lorsque vous dites que l'argument de la réputation ne tient pas face aux risques pour la sécurité nationale que présenterait la révélation de failles pour lesquelles on ne dispose pas de correctif.

Cela étant, je pense que nous devons suivre la rapporteure pour avis et considérer que les choses doivent rester en l'état dans la LPM, quitte à compléter ensuite le dispositif au niveau européen, avec la directive NIS 2 (Network and Information Security). On pourrait, par exemple, envisager un système de déclaration commun, sachant que certains logiciels commercialisés en France peuvent provenir d'éditeurs soumis au droit néerlandais. Il est donc important d'envisager des solutions de traitement de l'information coopératives, impliquant les différentes autorités nationales concernées, à l'instar de ce que nous avons fait avec le règlement général sur la protection des données (RGPD). En outre, dans le cadre européen, la menace de sanction est beaucoup plus forte du fait de l'extraterritorialité.

Sans être hostile sur le principe à la logique de ces amendements, je pense qu'il serait bon que nous soyons au clair sur les vulnérabilités, les *backdoors* – sans parler de Palentir, entouré d'une certaine opacité –, et que le bon vecteur en la matière est NIS 2. Si jamais la directive faisait l'impasse sur le sujet, alors nous l'inscririons dans le droit national afin de donner à l'Anssi un pouvoir de sanction administratif – je rejoins ici ce qu'a dit Ugo Bernalicis : les sanctions administratives ne sont pas l'apanage des autorités administratives indépendantes, comme le montre l'exemple de la DGCCRF. Cela étant, mieux vaut quand c'est une autorité administrative indépendante. (*MM. Éric Martineau, Mounir Belhamiti et Aurélien Lopez-Liguori applaudissent.*)

**Mme la présidente.** La parole est à Mme la rapporteure pour avis.

**Mme Sabine Thillaye, rapporteure pour avis.** Madame Thomin, je ne place absolument pas les intérêts commerciaux avant la défense et la sécurité nationale,...

**M. Erwan Balanant.** En effet, ce n'est pas ce que Mme la rapporteure pour avis a dit !

**Mme Sabine Thillaye, rapporteure pour avis.** ...j'ai simplement parlé d'équilibre. Une entreprise n'a aucun intérêt à commercialiser un produit défectueux, c'est du simple bon sens.

**M. Antoine Léaument.** Ce n'est pas vrai ! Même Philippe Latombe n'est pas d'accord avec vous !

**Mme Sabine Thillaye, rapporteure pour avis.** Nous voulons procéder par étapes, en appliquant d'abord le *name and shame* et, si ce n'est pas suffisant, en venir aux sanctions. Et puis, comme l'a dit notre collègue Latombe, beaucoup de sujets devront être traités au niveau européen.

**M. Laurent Jacobelli.** Nous voilà bien !

**Mme la présidente.** La parole est à M. le ministre délégué.

**M. Jean-Noël Barrot, ministre délégué.** J'apporte une précision à la représentation nationale avant le vote. Si elle pratique le *name and shame*, l'Anssi ne le fera pas en dévoilant à tous les vents la nature des failles d'un logiciel pour inviter tout le monde à s'y engouffrer ;...

**M. Philippe Latombe.** Heureusement !

**M. Jean-Noël Barrot, ministre délégué.** ...si une entreprise a omis de signaler des failles auprès de l'Anssi comme le prévoit l'article 34 de la loi de programmation militaire, celle-ci rendra simplement publique la vulnérabilité de tel logiciel, sans entrer dans les détails, afin de ne pas donner du grain à moudre à de potentiels assaillants.

(*Les amendements identiques n<sup>os</sup> 838 et 994 ne sont pas adoptés.*)

**Mme la présidente.** Je mets aux voix l'amendement n<sup>o</sup> 176.

(*Il est procédé au scrutin.*)

**Mme la présidente.** Voici le résultat du scrutin :

Nombre de votants .....	68
Nombre de suffrages exprimés .....	55
Majorité absolue .....	28
Pour l'adoption .....	13
contre .....	42

(*L'amendement n<sup>o</sup> 176 n'est pas adopté.*)

**Mme la présidente.** La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n<sup>o</sup> 175.

**Mme Mélanie Thomin.** Il propose une mesure d'efficacité. Le texte indique que, lorsqu'une faille survient dans le logiciel, les utilisateurs professionnels devront en être informés. Nous proposons la suppression du terme « professionnels », d'ailleurs ajouté en commission, car nous considérons que nos réseaux informatiques constituent une chaîne et que tous les utilisateurs, professionnels comme non professionnels, doivent être informés. Les ordinateurs des particuliers peuvent faire l'objet de contaminations et, à l'heure du télétravail, la sécurité des systèmes d'information devient l'affaire de tous, compte tenu de l'interconnexion des différents réseaux de communication. Il est donc dans l'intérêt

collectif que tout utilisateur, professionnel ou non professionnel, d'un logiciel présentant une faille de sécurité soit informé de celle-ci.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Si la commission a tenu à préciser que seuls étaient concernés les utilisateurs professionnels, c'est que ce sont précisément eux les acteurs ciblés par les dispositifs que nous instituons dans le cadre de la défense et de la sécurité nationale. Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis. Certains ont paru s'étonner que le Parlement amende les propositions initiales du Gouvernement.

**M. Antoine Léaument.** Perte d'habitude, sans doute !

**M. Jean-Noël Barrot, ministre délégué.** Mais il ne faut pas jeter la démocratie parlementaire avec l'eau du bain !

**M. Ugo Bernalicis.** Comme hier, en commission des affaires sociales, n'est-ce pas ?

**M. Erwan Balanant.** Oui, votre obstruction !

**M. Jean-Noël Barrot, ministre délégué.** Le Gouvernement présente un projet de loi, le Parlement s'en saisit ; la rapporteure pour avis et les membres de la commission ont mené des auditions pour confronter le texte du Gouvernement à l'épreuve du réel. Cela leur a permis d'en élaborer la rédaction et, en l'occurrence, d'apporter cette restriction aux seuls utilisateurs professionnels.

**M. Ugo Bernalicis.** Ce n'est pas la question !

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Je m'exprime sur cet amendement qui, s'il était adopté, ferait tomber le suivant.

Nous avons voulu, en commission des lois, cibler les utilisateurs professionnels de logiciel, mais la question se pose de leur définition : qu'entend-on par professionnels ? Incluent-ils, par exemple, les groupements hospitaliers de territoire (GHT), qui n'entrent pas nécessairement dans cette catégorie au sens du code de commerce, auquel on peut être susceptible de se référer pour interpréter l'article ?

En ce qui concerne néanmoins les particuliers, il existe déjà des dispositifs d'information publique, notamment parce que sont en jeu des données personnelles et que la Cnil est donc systématiquement avertie, que des procédures sont prévues et des sanctions possibles.

Dans le domaine de la sécurité nationale, qui nous intéresse ici, il faut être le plus rapide possible et donc privilégier en premier lieu l'information des professionnels déjà utilisateurs du logiciel, voire les entreprises d'infogérance qui utilisent des logiciels tiers et les modifient pour le compte d'autres professionnels.

La rédaction actuelle permet donc d'englober l'ensemble de la chaîne et d'aller le plus vite possible pour éviter que les failles de sécurité se démultiplient et soient massivement

utilisées. Quant aux particuliers, ils bénéficient d'autres canaux d'information, beaucoup plus précis et plus efficaces, que nous avons instaurés par souci d'efficacité.

*(L'amendement n° 175 n'est pas adopté.)*

**Mme la présidente.** La parole est à M. Philippe Latombe, pour soutenir l'amendement n° 1670.

**M. Philippe Latombe.** C'est un amendement d'appel, demandant que le Gouvernement précise bien ce que recouvre le terme « professionnels » et qu'on ne s'en tienne pas à la stricte définition du code de commerce.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Je laisserai le ministre répondre sur ce point et formulerai pour ma part une demande de retrait.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Monsieur Lacombe, je vous confirme que la rédaction est suffisamment générale pour couvrir tous les utilisateurs professionnels, qu'il s'agisse d'organisations privées ou publiques. En l'occurrence, les hôpitaux et les collectivités territoriales sont donc bien inclus dans le champ de l'article.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Il ne faut oublier personne car il y va de la portée de la coercition pouvant peser sur les éditeurs de logiciels. Puisque vous avez refusé les sanctions financières pour défaut de communication d'une vulnérabilité, il faut à tout le moins que les éditeurs en informent les utilisateurs ou, à défaut, l'Anssi.

Il ne faudrait donc pas que la rédaction actuelle rate la cible, et c'est la raison pour laquelle, en commission, je faisais partie de la minorité qui aurait préféré que l'on se réfère à tous les utilisateurs. Il n'y a pas toujours de consensus dans la fabrique de la loi, et il arrive que le débat recommence dans l'hémicycle, où le rapport de force n'est pas nécessairement le même qu'en commission – regardons ce qui s'est produit hier en commission des affaires sociales... Il me semble que vous tombez là dans votre propre piège, avec cette définition rabougrie. J'espère qu'il ne nous faudra pas une question prioritaire de constitutionnalité pour apprendre quelle est la définition exacte d'un professionnel.

*(L'amendement n° 1670 est retiré.)*

**Mme la présidente.** Sur l'article 34, je suis saisie par le groupe Démocrate (MODEM et indépendants) d'une demande de scrutin public.

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

La parole est à Mme Emmanuelle Ménard, pour soutenir l'amendement n° 847 rectifié.

**Mme Emmanuelle Ménard.** Mon intervention sera courte, car il s'agit d'un amendement très simple ayant pour objet de contraindre les éditeurs de logiciels à transmettre dans les plus brefs délais les informations nécessaires pour assurer la sécurité des données sensibles. L'amendement vise ainsi à introduire la notion d'immédiateté à l'article 34, en

imposant aux éditeurs d'agir « dès que » leurs produits sont affectés ou susceptibles de l'être par une vulnérabilité significative.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Même avis défavorable, ma chère collègue, que pour votre amendement n° 1121 qui visait à rendre automatiques les mesures prévues à l'article 32. Il convient en effet de laisser de la flexibilité à l'Anssi et aux éditeurs dans leur réponse aux actes malveillants.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à Mme Emmanuelle Ménard.

**Mme Emmanuelle Ménard.** Il me semble que les mots « dès que » laissent de la flexibilité, étant donné qu'ils ne veulent pas dire « à la seconde où ». Cet amendement me paraît de bon sens et contenir une formulation offrant une meilleure réponse aux préoccupations de sécurité vis-à-vis des éditeurs de logiciels.

*(L'amendement n° 847 rectifié n'est pas adopté.)*

**Mme la présidente.** Je suis saisie de deux amendements identiques, n° 1634 et 1673.

La parole est à Mme Clara Chassaniol, pour soutenir l'amendement n° 1634.

**Mme Clara Chassaniol.** Il vise à préciser que le délai d'information fixé par l'Anssi est pris selon certains critères, en l'occurrence les risques pour la sécurité nationale, l'urgence et le temps nécessaire pour prendre les mesures correctives. L'objectif est ici d'encadrer la décision de l'Anssi, afin de garantir que le délai d'information soit fixé non pas de manière discrétionnaire selon les éditeurs, mais bien de façon cohérente en fonction de certains critères, en vue d'un égal traitement des éditeurs par l'Anssi en matière d'obligations.

**M. Sylvain Maillard.** Très bien !

**Mme la présidente.** La parole est à M. Philippe Latombe, pour soutenir l'amendement n° 1673.

**M. Philippe Latombe.** En complétant les propos de notre collègue Chassaniol, je répondrai aussi à l'amendement n° 847 rectifié.

Nous avons une vraie difficulté de temporalité. S'il faut en effet que l'Anssi ne traite pas les éditeurs de manière discriminatoire, ce qui suppose un encadrement, il faut aussi qu'un correctif soit apporté à chaque vulnérabilité car, dans le cas contraire, des attaques seraient à même de s'en saisir : c'est ce que Mme Ménard soulevait en proposant l'ajout des mots « dès que ». Or, si nous avons besoin de correctifs, leur développement peut être plus ou moins long, ce qui nécessite de laisser de la souplesse à l'Anssi.

Par ailleurs, comme je viens de le dire, il nous faut aussi garantir que les décrets d'application de la loi interdiront tout traitement discriminatoire de la part de l'Anssi. Cette question a déjà été posée, certains éditeurs peuvent avoir des liens plus étroits ou des contacts plus nombreux avec l'Anssi, ou encore avoir des employés passés par cette agence,

ce qui pourrait leur permettre d'obtenir un traitement plus favorable, chose que nous cherchons donc à éviter par ces amendements. L'impératif est de nous assurer de l'applicabilité de la loi pour que les correctifs puissent être effectivement apportés. Il ne faudrait pas que des failles de vulnérabilité soient publiées dans un délai fixe, sans que les correctifs aient été apportés, car, le cas échéant, ce serait ouvrir la porte à des attaques coordonnées et massives que nous aurions pu éviter.

**Mme la présidente.** Quel est l'avis de la commission sur ces amendements identiques ?

**Mme Sabine Thillaye, rapporteure pour avis.** Il est favorable. Ces amendements s'inscrivent dans la continuité de nos travaux en commission et permettraient d'encadrer la fixation du délai d'information sans nuire à l'opérationnalité de la correction des vulnérabilités.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Je me suis exprimé tout à l'heure sur l'opportunité d'intégrer les risques pour la sécurité nationale parmi les critères d'appréciation, comme d'autres amendements sur d'autres articles ont également visé à le faire.

Par ailleurs, je tiens à souligner la pertinence des propos de M. Latombe : il convient de laisser à l'Anssi une marge d'appréciation dans sa prise de décision, plutôt que de la rendre automatique – ce que certains amendements tendent à faire –, afin de garantir, grâce à cette souplesse, l'efficacité du dispositif dont il est ici question et la protection des entités concernées.

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** Nous soutiendrons ces amendements visant à préciser les critères selon lesquels le délai d'information sera fixé.

Je souhaite également réagir aux propos de Mme la rapporteure pour avis, selon qui les entreprises n'ont pas intérêt à mettre des produits défectueux sur le marché. Pour avoir un peu travaillé dans le domaine du développement informatique, je puis vous dire qu'une très longue et très coûteuse phase de débogage suit le développement d'un logiciel. De nombreuses entreprises mettent donc sur le marché des produits en sachant pertinemment qu'ils comprennent des failles de sécurité très importantes.

**M. Antoine Léaument.** Exactement !

**M. Jérémie Iordanoff.** C'est par exemple l'habitude de Microsoft. Pour proposer des logiciels à des prix moins élevés, les éditeurs font pour ainsi dire accomplir le débogage par les utilisateurs, un signalement parvenant automatiquement aux entreprises après chaque dysfonctionnement et leur permettant de prendre connaissance des failles de sécurité. Le délai d'information dont nous parlons pourrait donc être très important, car la phase de débogage peut s'étendre sur un ou deux ans. Je le répète, pour des raisons économiques, les éditeurs n'ont pas toujours intérêt à mettre sur le marché des logiciels sûrs. *(Applaudissements sur quelques bancs du groupe LFI-NUPES.)*

**M. Antoine Léaument.** Même M. Latombe est d'accord !

*(Les amendements identiques n° 1634 et 1673 sont adoptés.)*

**Mme la présidente.** Je suis saisie de deux amendements identiques, n° 839 et 996.

La parole est à Mme Martine Etienne, pour soutenir l'amendement n° 839.

**Mme Martine Etienne.** Nous restons sur le même thème. Ces amendements visent à obliger l'Anssi à enjoindre aux éditeurs de logiciels d'informer leurs utilisateurs en cas de vulnérabilité ou d'incident compromettant la sécurité de leurs systèmes d'information.

Collègues, nous avons, tous, certainement, été déjà victimes de fuites de mot de passe, parfois même sans que nous en ayons été informés par les entreprises concernées. Or, aux termes du projet de loi, monsieur le ministre délégué, vous souhaitez qu'il soit simplement possible d'enjoindre aux éditeurs de logiciels de communiquer l'existence d'une faille. En ce qui nous concerne, nous estimons que ces derniers doivent être obligatoirement enjoins de le faire. J'insiste, l'Anssi doit systématiquement – et non éventuellement – rendre public un incident ou une vulnérabilité affectant la sécurité d'un produit lorsque son éditeur n'en informe pas ses utilisateurs. On ne doit pas jouer avec les données des citoyens et l'Anssi ne doit pas contribuer à ce Far West de la data dans lequel nous n'avons aucun contrôle.

**M. Manuel Bompard.** Excellent !

**Mme la présidente.** La parole est à M. Ugo Bernalicis, pour soutenir l'amendement n° 996.

**M. Ugo Bernalicis.** Nous sommes ici dans un cas de figure où une faille de vulnérabilité a été constatée et, je l'espère, communiquée à l'Anssi. Celle-ci doit donc, aux termes des amendements que nous venons d'adopter, fixer un délai à l'éditeur concerné pour qu'il fournisse un correctif et informe ses utilisateurs professionnels de cette faille. Voilà où nous en sommes. Or imaginons que, patatras, l'éditeur du logiciel ne fasse pas ce que lui a demandé l'Anssi : dans ce cas, l'Agence peut, je dis bien peut, c'est-à-dire éventuellement, faire elle-même ce que l'éditeur a refusé. Eh bien non ! Si l'Anssi a demandé à l'éditeur d'informer ses utilisateurs professionnels dans un certain délai, c'est qu'elle le jugeait utile, pertinent et nécessaire.

**M. Antoine Léaument.** Logique !

**M. Ugo Bernalicis.** Et si l'éditeur refuse d'agir, l'Anssi doit donc le faire à sa place. C'est d'ailleurs pour cette raison que l'entreprise comprendra qu'il vaut mieux agir elle-même, plutôt que d'être tributaire d'une communication de l'Anssi.

J'insiste, la possibilité d'agir à la place de l'éditeur n'est pas suffisante, surtout eu égard à ses capacités de négociation – ce qui nous fait revenir à la discussion précédente –, celles-ci dépendant de la taille de l'entreprise, de ses relations avec l'Anssi, voire avec l'État, ou encore de la présence en son sein de personnes ayant travaillé à l'Anssi par le passé : les choses de la vie, en somme. Voilà pourquoi nous préférierions nous prémunir contre la décision potentiellement arbitraire de publier ou de ne pas publier une vulnérabilité, alors même que l'Anssi – une fois de plus je ne fais que reprendre les termes du texte et des amendements que nous examinons – aurait déjà enjoint à l'éditeur de le faire.

**Mme la présidente.** Quel est l'avis de la commission sur ces amendements identiques ?

**Mme Sabine Thillaye, rapporteure pour avis.** J'estime pour ma part qu'une publication obligatoire rigidifierait trop le texte. Comme précédemment, il faut laisser un peu de latitude à l'Anssi pour apprécier les vulnérabilités et prendre ses décisions en conséquence. En commission,

nous avons adopté un amendement de notre collègue Belhamiti visant à ce que le délai d'information des utilisateurs soit déterminé par l'Anssi. Et nous venons d'adopter les amendements n°s 1634 et 1673 qui viennent préciser que ce délai dépend de l'urgence, des risques pour la sécurité nationale – je rappelle à nouveau que nous examinons une LPM – et du temps nécessaire aux éditeurs pour prendre les mesures correctives. Il est préférable d'apprécier concrètement ce qu'il convient de faire, en fonction de l'ampleur de l'incident et de la vulnérabilité. J'émet donc un avis défavorable sur ces amendements identiques.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Je ne résiste pas, madame la présidente, à la tentation de réagir aux propos de Mme la rapporteure pour avis, selon qui les obligations obligatoires sont tout de même rigides. (*Sourires sur les bancs des groupes LFI-NUPES et Écolo-NUPES.*) J'en conviens, les obligations facultatives sont plus souples. Je ne savais pas que nous étions en cours de yoga parlementaire ! (*Mêmes sourires.*) Une chose est sûre : je dois encore travailler ma souplesse.

**M. Erwan Balanant.** Souplesse intellectuelle surtout !

**M. Ugo Bernalicis.** Une fois de plus, votre raisonnement ne tient pas. Nous sommes dans le cas où un éditeur, après avoir été enjoint par l'Anssi d'avertir dans certains délais ses utilisateurs professionnels d'une vulnérabilité et de fournir le correctif adapté, ne le fait pas. Or si elle le lui a demandé, c'est que c'était pertinent, ou alors c'est que quelque chose ne tourne pas rond dans ma tête ou dans le raisonnement.

**M. Laurent Jacobelli.** On peut effectivement en discuter !

**M. Ugo Bernalicis.** Si l'Anssi a estimé pertinent d'enjoindre à une entreprise d'informer ses utilisateurs d'une faille et que cette entreprise fait défaut, il faut que cette communication soit obligatoirement faite par l'Agence car, dans le cas contraire, votre dispositif ne serait qu'un pétard mouillé !

**M. Laurent Jacobelli.** Ça, il faut le dire à M. Boyard !

**M. Ugo Bernalicis.** Le dispositif ne servirait à rien ! Dès lors, autant ne rien prévoir du tout, car cela reviendrait au même. Les choses ne relèveraient alors que du dialogue normal entre une administration et ses usagers et il existe déjà un code des relations entre le public et l'administration. J'insiste : pourquoi alourdirions-nous la loi avec des dispositions indiquant que les gens peuvent discuter entre eux ? Ils le peuvent évidemment.

Il convient donc de verrouiller les choses formellement. Une marge d'appréciation est déjà laissée à l'Anssi dans le début de l'alinéa 6 : au bout du compte, il faut tout de même prévoir un couperet. Vous avez refusé l'introduction de sanctions financières, monsieur le ministre délégué, au motif que les entreprises font déjà face à un risque réputationnel, mais si ce dernier peut être lui-même sujet à discussion et à négociation, je répète qu'il n'y a plus rien ! Chacun fait alors comme il veut, à la bonne franquette, en fonction de son entregent et de son réseau, notamment dans les administrations.

Je ne suis pas d'accord avec les obligations facultatives. Si vous voulez faire du yoga, il y a des cours bien meilleurs qu'à l'Assemblée nationale.

**Mme la présidente.** La parole est à M. le ministre délégué.

**M. Jean-Noël Barrot, ministre délégué.** Nous commençons à faire le tour du débat. En réalité, les choses ne sont pas aussi simples que vous le dites. Cela a été évoqué, des questions se posent au sujet des mesures correctives, sachant que des problèmes de coordination entre éditeurs peuvent aussi avoir lieu, ce qui suppose donc que des marges d'appréciation soient laissées à l'Anssi au moment de donner une injonction à une entreprise.

**M. Ugo Bernalicis.** C'est déjà réglé par le début de l'alinéa 6 !

**M. Jean-Noël Barrot, ministre délégué.** Si ce n'est déjà fait, je vous invite à auditionner les représentants de l'Anssi, car celle-ci fait montre d'une grande diligence, d'une grande réactivité chaque fois qu'elle est informée d'attaques contre les autorités, les OIV – opérateurs d'importance vitale –, les OSE – opérateurs de services essentiels. Ainsi enjoindra-t-elle à un éditeur d'informer sur une vulnérabilité dont elle aurait eu connaissance et qui le nécessiterait,...

**M. Ugo Bernalicis.** Mais si l'éditeur ne le fait pas ?

**M. Jean-Noël Barrot, ministre délégué.** ...sachant que, à défaut, elle pourra exercer cette capacité qui lui est conférée de faire elle-même la publicité de la vulnérabilité en question. J'estime que nous avons ainsi un ensemble cohérent, suffisamment contraignant, car impliquant un risque réputationnel pour les éditeurs, qui seront incités à répondre aux injonctions de l'Anssi, tout en laissant des marges d'appréciation suffisantes à l'Agence pour ne pas aggraver la situation lorsque survient une vulnérabilité.

**M. Ugo Bernalicis.** C'est déjà résolu par le début de l'alinéa 6 !

*(Les amendements identiques n<sup>os</sup> 839 et 996 ne sont pas adoptés.)*

**Mme la présidente.** La parole est à M. Aurélien Lopez-Liguori, pour soutenir l'amendement n<sup>o</sup> 1613.

**M. Aurélien Lopez-Liguori.** L'article 34 vise à permettre à l'Anssi de publier les vulnérabilités d'une entreprise. Il s'agit non seulement d'une méthode contestable, mais qui est, en outre, de nature à mettre en danger une entreprise en l'exposant potentiellement à d'autres attaques. En effet, ce serait une occasion en or pour les hackers : on leur offrirait sur un plateau d'argent une voie d'entrée dans les systèmes d'information. Ils s'en donneraient à cœur joie, puisqu'il leur suffirait de consulter les publications de l'Anssi pour disposer d'une liste d'entreprises vulnérables sur lesquelles concentrer leurs attaques.

Si je comprends votre volonté d'inciter les entreprises à combler les failles de leurs systèmes, vous faites en réalité peser une épée de Damoclès au-dessus de leur tête. Le *name and shame* prôné par Mme la rapporteure pour avis ressemble plus à une méthode de hackers qu'à la réponse qu'un État de droit devrait apporter au problème : elle n'est pas digne d'un organisme dépendant du Premier ministre. Dans un État de droit, la constatation d'un manquement donne lieu à une sanction.

Mon amendement vise à empêcher la publication par l'Anssi de la liste des entreprises présentant des vulnérabilités significatives avant qu'elles n'aient pu y remédier, la publication étant au mieux contre-productive, au pire dangereuse, puisque les failles pourraient alors être exploitées. Afin d'assurer la pénalisation des entreprises qui ne signaleraient

ou ne combleraient pas leurs failles, j'ai déposé un amendement après l'article 36 prévoyant que le Gouvernement remet au Parlement un rapport portant notamment sur la définition de sanctions applicables en cas de manquement des éditeurs. Nos collègues de la NUPES proposaient une amende à hauteur de 4 % du chiffre d'affaires : nous envisageons, pour notre part, une sanction proportionnelle. Un rapport nous permettra d'identifier la sanction la plus pertinente.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Attendre que la vulnérabilité soit résorbée annulerait tout l'intérêt du dispositif,...

**M. Aurélien Lopez-Liguori.** C'est le but !

**Mme Sabine Thillaye, rapporteure pour avis.** ...dont l'objectif est d'informer les utilisateurs de la présence d'une faille dans le logiciel afin d'en limiter les victimes. Il est bien entendu que, parallèlement à cette publication, l'Anssi, en lien avec l'éditeur victime de l'attaque, travaille à combler la faille. Votre amendement conduisant à affaiblir le dispositif, j'émettrai un avis défavorable.

**M. Aurélien Lopez-Liguori.** D'où ma proposition en matière de pénalisation !

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Tout à l'heure, l'Assemblée a rejeté des amendements qui prévoyaient que l'Anssi publie systématiquement la liste des entreprises présentant des vulnérabilités. Comme Mme la rapporteure pour avis, j'ai alors indiqué que, pour faire échec à la menace, il pouvait parfois être plus habile et intelligent de ne pas dévoiler les failles, ou de ne le faire que partiellement. Conserver une marge d'appréciation me semblait important. En empêchant toute publication tant que les failles ne sont pas comblées, votre amendement risque d'encourager les éditeurs, dont la réputation n'est alors plus compromise, à ne pas mettre tout en œuvre pour y remédier – c'est aussi le revers de la médaille du rejet des amendements précédents. Pour cette raison, j'y suis défavorable.

**Mme la présidente.** La parole est à M. Aurélien Lopez-Liguori.

**M. Aurélien Lopez-Liguori.** Je comprends votre argument, monsieur le ministre délégué. Il est bien évident que, seul, cet amendement ne permet pas d'inciter les éditeurs à signaler et combler les failles de leurs systèmes, et c'est pour cette raison que j'ai déposé après l'article 36 un amendement tendant à demander un rapport sur la pénalisation des entreprises qui ne répondraient pas aux demandes de l'Anssi. La réponse d'un État de droit à ce type de manquements doit être une sanction, pas le *name and shame* proposé par Mme la rapporteure pour avis.

*(L'amendement n<sup>o</sup> 1613 n'est pas adopté.)*

**Mme la présidente.** La parole est à Mme Anne Le Hénauff, pour soutenir l'amendement n<sup>o</sup> 995.

**Mme Anne Le Hénauff.** Dans un souci de clarté et d'identification des acteurs concernés, il convient d'apporter un éclairage sur la notion d'éditeur de logiciel. Dès lors que son activité correspond à la définition suivante, nul ne pourra prétendre se soustraire aux dispositions du présent article : « On entend par éditeur de logiciel toute personne

physique ou morale qui conçoit ou développe un produit logiciel ou fait concevoir ou développer un produit logiciel, et le met à disposition d'utilisateurs, à titre onéreux ou gratuit. » Cette définition traduit la jurisprudence rendue en la matière.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** La première définition que vous aviez proposée lors des débats en commission n'était pas pleinement satisfaisante. Cette nouvelle rédaction me paraît beaucoup plus robuste et complète : avis favorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Même avis.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Il était absolument nécessaire de définir la notion d'éditeur de logiciel, et je regrette que nous ayons manqué d'occasions de le faire plus tôt, d'autant que la LPM n'est pas le meilleur véhicule législatif. Cette définition, qui sédimente la jurisprudence en la matière, est le fruit d'un beau travail légistique et sera utile pour d'autres textes, puisqu'elle permettra notamment d'imposer des obligations ou de fournir des moyens aux éditeurs de logiciels et facilitera la transposition dans le droit national de textes européens, comme la directive NIS 2.

*(L'amendement n° 995 est adopté.)*

**Mme la présidente.** La parole est à M. Laurent Jacobelli, pour soutenir l'amendement n° 1037.

**M. Laurent Jacobelli.** Le débat montre bien la nécessité de définir ou de préciser les contours de l'article. L'amendement vise à préciser l'alinéa 8 en révoquant qu'un référentiel définira les critères permettant « l'évaluation objective » – j'insiste sur ce terme – « du caractère significatif » des vulnérabilités et incidents, l'article ne faisant référence, en l'état, qu'à « des standards internationaux communément admis ». Il semble en effet difficile de demander à des entreprises de respecter certains critères de protection sans que ceux-ci soient clairement définis.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** L'amendement tend à réécrire un alinéa que j'ai déjà complété en commission : l'exposé des motifs de mon amendement précisait que parmi les standards internationaux figure le CVSS – système standardisé de notation de vulnérabilité.

**M. Laurent Jacobelli.** Ce n'est pas écrit dans le texte !

**Mme Sabine Thillaye, rapporteure pour avis.** La rédaction actuelle me paraît équilibrée et suffisamment précise : avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Mme la rapporteure pour avis a rappelé à raison que des précisions avaient d'ores et déjà été apportées en commission. Néanmoins, un élément encore mériterait effectivement d'être précisé : si les critères de vulnérabilité sont effectivement encadrés par des standards internationaux, il n'existe aucune caractérisation communément admise des incidents. L'amendement suivant, déposé par Mme la rapporteure pour avis, vise à préciser que les standards internationaux ne servent donc de grille d'évalua-

tion que pour les vulnérabilités. Afin d'aboutir à la meilleure rédaction possible de l'article 34, je vous demande donc de bien vouloir retirer votre amendement au bénéfice de l'amendement n° 1217 de Mme la rapporteure pour avis.

*(L'amendement n° 1037 n'est pas adopté.)*

**Mme la présidente.** La parole est à Mme la rapporteure pour avis, pour soutenir l'amendement n° 1217.

**Mme Sabine Thillaye, rapporteure pour avis.** La notion de standards internationaux n'étant pertinente qu'en matière de vulnérabilités, mon amendement tend, comme l'a indiqué M. le ministre délégué, à préciser qu'ils ne s'appliquent pas aux incidents.

*(L'amendement n° 1217, accepté par le Gouvernement, est adopté.)*

**Mme la présidente.** Je mets aux voix l'article 34.

*(Il est procédé au scrutin.)*

**Mme la présidente.** Voici le résultat du scrutin :

Nombre de votants .....	85
Nombre de suffrages exprimés .....	83
Majorité absolue .....	42
Pour l'adoption .....	81
contre .....	2

*(L'article 34, amendé, est adopté.)*

### **Suspension et reprise de la séance**

**Mme la présidente.** La séance est suspendue.

*(La séance, suspendue à onze heures vingt-cinq, est reprise à onze heures quarante.)*

**Mme la présidente.** La séance est reprise.

### **Article 35**

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** Lorsque, en commission, nous avons commencé l'examen de l'article 35, nous étions très défavorables à sa rédaction. Nos amendements ont notamment permis de circonscrire son application « aux seules fins de garantir la défense et la sécurité nationale » – précision indispensable, de même que le maintien, pour les agents de l'Anssi recueillant des données auprès des acteurs numériques, de la nécessité d'être assermentés, disposition dont l'article prévoyait initialement la suppression. Ainsi modifié, il est désormais acceptable, conforme à ce qu'il doit être, si bien que nous voterons contre les amendements identiques tendant à le supprimer.

En revanche, monsieur le ministre délégué, il ressort de cet article que des traceurs et balises peuvent être placés « sur le système d'information [...] d'un opérateur de centre de données affecté par la menace ». Or de plus en plus de centres de données sont en colocation, c'est-à-dire louent de l'espace à des tiers, ce qui pose une question d'extraterritorialité : les dispositifs permettant le recueil de données porteront-ils bien seulement sur le système d'information, par opposition aux *meet-me rooms* (MMR) du centre, voire

à ses locataires, qui peuvent relever d'un droit extra-européen? Il importe de confirmer que nous sommes d'accord sur ce point pour fixer la portée de l'article et ne pas risquer de créer un précédent, notamment à l'égard des entreprises françaises qui auraient besoin, aux États-Unis ou ailleurs, de solutions analogues.

**Mme la présidente.** La parole est à Mme Anne Le Hénauff.

**Mme Anne Le Hénauff.** L'article 35 prévoit de renforcer les capacités de détection des cyberattaques et l'information des victimes par divers moyens : recueil de données sur le réseau d'un opérateur de communications électroniques ou le système d'information d'un fournisseur d'accès, d'un hébergeur, d'un centre de données ; obligation pour les OIV de disposer d'un système de détection des attaques informatiques ; obligation pour les hébergeurs de données de communiquer à l'Anssi certaines informations relatives aux utilisateurs ou systèmes d'information vulnérables, menacés ou attaqués.

Étant donné l'octroi à l'Anssi de ces nouvelles prérogatives, il est nécessaire de s'assurer de l'encadrement des dispositifs en cause : c'est pourquoi le groupe Horizons et apparentés se félicite que l'adoption en commission de deux de ses amendements ait garanti, d'une part, que la collecte de données par l'Anssi n'aura lieu qu'à des fins de défense et de sécurité nationale ; d'autre part qu'elle n'incombera qu'à des agents habilités et, comme le dispose le code de la défense, assermentés. Tout en demeurant vigilants, quant aux amendements proposés, en matière de clarification et de précision, nous voterons en faveur de l'article.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Les nouveaux pouvoirs de l'Anssi ressemblent bizarrement à ce qui se pratique en matière de renseignement : la captation de données par des boîtes noires. Certes, le mécanisme prévu par le texte est plus circonscrit, mais je ne m'en pose pas moins des questions. Sa finalité serait plutôt préventive : on nous explique qu'il ne sera mis en œuvre que tant que durera la menace, et dans le même temps que, l'Anssi ne roulant pas sur l'or, les dispositifs techniques pourraient être installés et analysés par les opérateurs eux-mêmes.

Ces opérateurs auront donc à leur main un dispositif technique de captation de leurs propres données, à des fins d'analyse, alors que, pour des raisons de préservation des données personnelles des utilisateurs, ils ne sont théoriquement pas censés réaliser ces captations. Il y a donc plusieurs éléments gênants dans cet article, même si ces dispositions sont prises au motif de la sécurité nationale. Le groupe LFI-NUPES désapprouve l'attribution de nouvelles compétences et prérogatives à l'Anssi, en particulier sur le périmètre mentionné. La délégation possible de l'exploitation du dispositif de marqueurs techniques à l'opérateur porte, selon nous, une atteinte forte à la souveraineté et à la préservation des données.

**Mme la présidente.** Je suis saisie de trois amendements identiques, n<sup>os</sup> 177, 840 et 997, tendant à supprimer l'article 35.

La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n<sup>o</sup> 177.

**Mme Mélanie Thomin.** Cet amendement d'appel vise à maintenir les missions de l'Anssi dans leur cadre actuel. Le groupe Socialistes et apparentés a, en effet, pointé plusieurs risques majeurs depuis le début des débats. Ces risques

concernent les délais de conservation des données, la capacité de contrôle donnée à l'Arcep, autorité indépendante en laquelle nous plaçons évidemment nos espoirs, et l'absence de précisions concernant le recours au juge administratif suivant la procédure du référé-liberté.

Or nous constatons que les garanties que nous vous proposons depuis le début de nos débats ne sont jamais retenues. L'extension des pouvoirs de l'Anssi revêt donc une portée incertaine en termes de capacité et de moyens. Elle pourrait être bénéfique mais, lorsque nous pointons de réels sujets d'inquiétude en matière de droits et de libertés, vous ne faites pas preuve d'esprit de coopération. Nous avons, en revanche, le sentiment que vous montrez une certaine complaisance à l'égard du monde économique, au détriment de nos enjeux de sécurité. La défense du présent amendement de suppression nous donne l'occasion d'appeler à la vigilance non seulement les citoyens mais aussi le Conseil constitutionnel.

**Mme la présidente.** La parole est à M. Antoine Léaument, pour soutenir l'amendement n<sup>o</sup> 840.

**M. Antoine Léaument.** Celui-ci n'est pas un amendement d'appel, c'est bien un amendement de suppression de l'article ! Nous considérons en effet que l'article 35 élargit dans une trop grande mesure les pouvoirs donnés à l'Anssi et désapprouvons surtout – c'est le point le plus problématique pour nous – le fait que ce soient les opérateurs qui placent des dispositifs de collecte de données puis les transmettent, sur saisie de l'Anssi. Cela nous semble illogique, d'autant plus que d'autres modes de fonctionnement pourraient sans doute être envisagés.

Je profite de l'occasion pour vous signaler dès à présent un problème de cohérence dans le texte : à l'alinéa 13, il est indiqué « Ces données ne peuvent être exploitées qu'aux seules fins de caractériser la menace affectant la sécurité de ces systèmes, à l'exclusion de toute autre exploitation. Elles ne peuvent être conservées plus de dix ans. »

**M. Jean-Noël Barrot, ministre délégué.** Jusqu'à l'amendement n<sup>o</sup> 180 de Mme Thomin !

**M. Antoine Léaument.** Je sais bien qu'un amendement à venir pourrait modifier la durée ! Je me permettais simplement de signaler, de façon un peu habile, que l'on en revient à l'incohérence signalée précédemment s'agissant de la conservation des données.

**Mme la présidente.** La parole est à M. Ugo Bernalicis, pour soutenir l'amendement n<sup>o</sup> 997.

**M. Ugo Bernalicis.** Alinéa après alinéa, l'article 35 pose problème en de multiples endroits ! Le dispositif est censé être préventif, alors qu'il est circonscrit à l'existence d'une menace, ce qui est contradictoire. Des garanties sont données quant à la durée des mesures – on parle à l'article 32 de deux mois – et quant à la nécessité de les reconduire, mais elles ne correspondent pas à la logique préventive qui est affichée. Les marqueurs techniques devant capter les données ne sont pas précisément définis. On nous indique que les données personnelles seront détruites, car ce ne sont pas celles que l'on recherche mais, encore une fois, comment faire la distinction entre ce qui est personnel et ce qui ne l'est pas ? Ce n'est pas toujours aussi évident qu'on veut bien le croire. Les données seront conservées cinq ans et non pas dix si, comme je l'imagine, l'amendement de Mme Thomin est adopté tout à l'heure par cohérence – bien que nous ne soyons pas à l'abri d'une incohérence !

Par ailleurs, les fournisseurs d'accès à internet exploiteront eux-mêmes les captations de données qu'ils auront réalisées sur commande de l'Anssi et, cerise sur le gâteau, le texte mentionne encore les surcoûts : il ne faudrait tout de même pas que la sécurisation des systèmes d'information coûte de l'argent aux opérateurs !

Tout cela n'est pas acceptable ! Vous ne pouvez pas élargir les prérogatives de l'Anssi sans nous démontrer la nécessité de le faire. En théorie, lorsque l'on prend des mesures attentatoires à plusieurs libertés – y compris celle d'entreprendre –, on explique pourquoi et l'on ne se contente pas d'évoquer une éventuelle menace ! Nous réfutons non seulement l'objectif de l'article 35 mais aussi ses dispositions concrètes : à mesure que l'on égrène les alinéas, de nouveaux problèmes surgissent. Nous demandons donc sa suppression et refusons que les prérogatives actuelles de l'Anssi soient élargies.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Il ne me semble pas inutile de rappeler l'objectif de l'article 35, les garanties prévues dès la version originale du texte et celles qui ont été introduites en commission des lois. L'article 35 vise à compléter le dispositif actuel qui permet déjà à l'Anssi, depuis la dernière loi de programmation militaire, de recourir à des marqueurs techniques pour obtenir, pendant une durée limitée, des informations sur les flux entrants et sortants d'une machine contrôlée par un cyberattaquant lorsque cette attaque constitue une menace pour les intérêts du pays. La collecte de ces informations purement technique est utile mais suppose que l'Anssi connaisse en amont les modes opératoires utilisés par les attaquants. Cet article vise ainsi à rendre possible le renforcement des capacités de détection d'attaques à l'encontre des systèmes d'information des autorités publiques et des opérateurs stratégiques en permettant à l'Anssi, en cas de menace grave, de mettre en œuvre des dispositifs de recueil de données.

Je peux comprendre que ces dispositifs interrogent et que l'on ait besoin de garanties. L'Anssi estime qu'environ cinquante copies de serveurs pourraient être faites par an, ainsi qu'une vingtaine de captations de flux réseau : ces chiffres paraissent proportionnés au regard de l'objectif de lutte contre les menaces sur la sécurité nationale.

J'en viens aux garanties prévues. Il y a d'abord un ciblage préalable de la machine compromise faisant objet de la copie : concrètement, l'Anssi devra motiver sa demande. Est ensuite prévu un contrôle de l'application de ces nouvelles mesures par l'Arcep, qui sera saisie en amont de tout enclenchement du dispositif et pourra, si elle l'estime fondé, refuser à l'Anssi l'engagement de la procédure. Par ailleurs, la durée de conservation des données utiles a été réduite à deux ans au lieu de dix ans dans le dispositif actuel, et les demandes ne portent que sur le périmètre d'opérateurs présentant une sensibilité particulière – autorités publiques, OIV, OSE – pour une durée limitée et avec pour finalité la prévention et la caractérisation des menaces. Les données ne seront obtenues et exploitées que par des agents individuellement désignés et spécialement habilités, et la destruction immédiate des données par l'Anssi est prévue par notre droit.

La commission de lois a introduit des garanties supplémentaires, d'une part en exigeant des précisions sur le type de données faisant l'objet d'un recueil, d'autre part en prévoyant la consultation de la Cnil avant la publication du décret. Elle a également maintenu l'assermentation des agents chargés de

l'opération de recueil et circonscrit l'utilisation de l'article aux situations les plus graves, menaçant la défense et la sécurité nationale.

Pour toutes ces raisons, estimant que nous sommes parvenus à un équilibre, j'émet un avis défavorable sur les amendements de suppression de l'article.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Mme la rapporteure pour avis a bien rappelé l'objectif poursuivi par l'article et les améliorations apportées en commission ; je n'y reviendrai pas. Je voudrais simplement souligner que, comme vous le savez, ce dispositif trouve son origine dans les leçons tirées du dispositif prévu par la loi de programmation militaire précédente. Deux raisons expliquent la rédaction de cet article. D'abord, il était déjà prévu que l'Anssi puisse donner des marqueurs techniques, c'est-à-dire des adresses IP, aux opérateurs de communications électroniques qui sont eux-mêmes opérateurs d'importance vitale, si ces derniers en manifestaient la volonté. Or l'expérience a montré qu'un seul de ces opérateurs était entré dans une démarche de coopération active avec l'Anssi. C'est ainsi qu'est née l'idée de rendre cette coopération obligatoire.

Deuxièmement, l'évolution de la menace a conduit à proposer que l'Anssi, après avoir sollicité l'avis conforme de l'Arcep – les travaux en commission ayant permis d'affiner le dispositif de contrôle –, de placer des balises devant des serveurs compromis ou utilisés pour mener des attaques à l'encontre des autorités, des OIV et des OSE. Ces balises ne pourront donc être posées que sur des serveurs physiquement localisés sur le territoire national, de telle sorte que cette mesure ne présente pas de caractère extraterritorial.

S'agissant du point soulevé par M. Latombe, le dialogue engagé par l'Anssi avec les détenteurs des équipements, sous le contrôle de l'Arcep, permettra de résoudre les problèmes de colocation et de placer la balise de telle sorte qu'elle ponctionne le moins de données possible des serveurs.

**Mme la présidente.** La parole est à Mme Anne Le Hénanff.

**Mme Anne Le Hénanff.** Remettons les choses dans la perspective du projet de loi de programmation militaire. L'évolution des prérogatives accordées à l'Anssi suit l'évolution des menaces. En effet, trois nouveaux terrains de conflictualité ont été largement pris en compte par le projet de LPM : les fonds marins, l'espace et le cyber. Il est donc tout à fait normal, et même rassurant, de savoir que nous adaptons les nouvelles prérogatives de l'Anssi à ces nouveaux terrains de conflictualité.

Il est choquant, par ailleurs, de sous-entendre que l'évolution des prérogatives accordées à l'Anssi serait une atteinte à la souveraineté nationale. L'Anssi, en tant que telle, représente justement, en lien avec la Première ministre, une garantie de l'autonomie stratégique de la France, de sa souveraineté numérique et de sa souveraineté nationale. Sans doute est-il nécessaire de le rappeler tant il est choquant, je le répète, de sous-entendre que l'Anssi pourrait, d'une manière ou d'une autre, attenter à la souveraineté nationale.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Ce n'est pas ce que j'ai dit, chère collègue.

**Mme Anne Le Hénanff.** Si, c'est ce que vous avez dit.

**M. Ugo Bernalicis.** Non, non ! J'ai dit que le fait de confier la gestion de marqueurs fournis par l'Anssi à des opérateurs privés qui ne sont précisément pas l'Anssi peut soulever un problème de souveraineté. Je souhaiterais que ces marqueurs, s'ils sont mis en œuvre, soient tous gérés par l'Anssi et ses services, c'est-à-dire par le service public. Voilà ce que je dis ! Encore une fois, on va à l'économie parce que l'on n'a pas suffisamment de moyens, même s'il n'y a jamais que cinquante objectifs, et l'on préfère passer par les opérateurs privés. Or des individus pourraient s'introduire dans les locaux de ces derniers et découvrir ainsi, grâce aux marqueurs qui y sont exploités, les cibles et les objectifs de l'Anssi.

Les explications du ministre délégué sont intéressantes s'agissant des objectifs, des opérateurs d'importance vitale et des balises posées devant les serveurs pour contrer les intrusions. Mais il s'agit d'un autre aspect du dispositif, qui pose beaucoup moins de problèmes. Les opérateurs voient un intérêt immédiat et direct à collaborer avec les services de l'Anssi et à bénéficier de ses capacités techniques. Les deux aspects du dispositif nous sont présentés comme indissociables, mais ils ne le sont pas ! Je répète que le dispositif présente une incohérence, qu'il vise deux objectifs qui ne sont pas identiques et que l'on essaye de nous faire avaler l'un avec l'autre.

*(Les amendements identiques n<sup>os</sup> 177, 840 et 997 ne sont pas adoptés.)*

**Mme la présidente.** La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n<sup>o</sup> 1271.

**M. Jérémie Iordanoff.** Avec cet amendement, je reviens une nouvelle fois sur la notion de sécurité nationale. Par dérogation, le droit de l'Union européenne autorise les États membres à utiliser les données de connexion de leurs ressortissants pour préserver la sécurité nationale mais la Cour de justice de l'Union européenne (CJUE) retient une conception très stricte de cette notion.

Nous avons eu plusieurs fois le débat mais vous nous avez renvoyés, monsieur le ministre délégué, à la décision du Conseil constitutionnel, sans donner la liste de ce que recouvre cette notion. Il me semble que les hôpitaux et les collectivités locales n'en font pas partie et que cette définition ne correspond toujours pas à ce qui est attendu par l'Anssi. Pour garantir les libertés de nos concitoyens, nous avons besoin d'une définition de ce qu'on entend par sécurité nationale.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Nous avons eu ce débat lors de l'examen des articles précédents. Avis défavorable.

*(L'amendement n<sup>o</sup> 1271 n'est pas adopté.)*

**Mme la présidente.** L'amendement n<sup>o</sup> 1047 de M. Frank Giletti est défendu.

*(L'amendement n<sup>o</sup> 1047, repoussé par la commission et le Gouvernement, n'est pas adopté.)*

**Mme la présidente.** Sur l'article 35, je suis saisie par le groupe Renaissance et le groupe Démocrate (MODÈM et indépendants) d'une demande de scrutin public.

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

La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n<sup>o</sup> 178.

**Mme Mélanie Thomin.** La mise en œuvre de marqueurs techniques doit être soumise à un avis conforme de l'Arcep. Cette autorité administrative connaît bien notre infrastructure informatique, elle est par ailleurs un gage de sérieux et d'indépendance pour contrôler le respect de l'État de droit.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Contrairement aux dispositifs visés à l'alinéa 5, les éléments que l'Anssi recueillera sur le réseau d'un OCE – opérateur de communications électroniques –, par ailleurs opérateur d'importance vitale, ne sont pas des données de contenu mais des adresses IP. Lorsque cette possibilité a été donnée en 2018, sur une base volontaire, c'est un contrôle *a posteriori* de l'Arcep qui a été prévu : le Conseil d'État a alors jugé la disposition suffisante, estimant que le contrôle était proportionné. Son avis n'a pas varié s'agissant de l'article 35 de la LPM, qui impose en outre la coopération entre les OCE et l'Anssi.

**Mme la présidente.** La parole est à M. Antoine Léaument.

**M. Antoine Léaument.** Une nouvelle fois, j'ai du mal à comprendre pourquoi cet avis de l'Arcep vous pose problème. Certes, il doit être possible de déroger à certains droits, mais uniquement lorsque les intérêts fondamentaux de la nation, la sécurité intérieure sont en jeu. Mélanie Thomin propose simplement que la disposition soit soumise à un avis préalable et conforme de l'Arcep.

S'assurer que les droits sont garantis n'est pas une mince affaire. Prenons l'article 66 de la Constitution, que chacun devrait apprendre par cœur : « Nul ne peut être arbitrairement détenu. » Pour qu'un tel droit soit garanti, il faut des moyens matériels. Sans moyens et sans autorité indépendante dans le processus de décision, les droits prévus dans la Constitution et la Déclaration des droits de l'homme et du citoyen ne sont pas effectifs. En ajoutant un acteur supplémentaire dans la prise de décision, l'amendement permet à une autre autorité de garantir les droits en donnant son avis. La garantie des droits contre l'arbitraire, je le répète, est la question centrale qui a présidé à la fondation de la nation en 1789. Si nous voulons faire les choses correctement, la garantie des droits doit être la priorité, pas un élément secondaire.

*(L'amendement n<sup>o</sup> 178 n'est pas adopté.)*

**Mme la présidente.** La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n<sup>o</sup> 1276.

**M. Jérémie Iordanoff.** Les alinéas 5 à 8 donnent à l'Anssi la possibilité de capturer l'intégralité d'un trafic réseau – et non plus seulement les données techniques – ou de copier la totalité d'un serveur pour y rechercher des informations caractérisant une menace. Si nous proposons de supprimer ce dispositif, c'est pour deux raisons.

D'abord, il n'est pas nécessaire de légiférer puisque l'Anssi dispose déjà de larges pouvoirs d'investigation, sous le contrôle de l'autorité judiciaire. C'est en tout cas ce que révèle le Gouvernement dans l'étude d'impact : pour illustrer l'utilité de l'accès de l'Anssi au contenu des machines infectées, il explique que le parquet a ouvert en 2017 une enquête de flagrance, permettant à l'Anssi de procéder à l'analyse d'un serveur. Celle-ci a permis d'identifier non seulement les victimes mais aussi les autres cibles de l'attaquant – elles étaient répertoriées sur le serveur. Il est question non pas de nier les prérogatives de l'Anssi mais de réclamer que l'autorité judiciaire continue d'exercer son contrôle.

Cela nous amène à la seconde raison : le dispositif présente un risque majeur pour les libertés publiques. Certes, des garde-fous sont prévus : l'Anssi ne peut prendre ses décisions qu'après avoir recueilli l'avis conforme de l'Arcep. Pourtant, dans son avis du 9 mars 2023, l'Arcep explique qu'elle ne dispose pas des moyens d'exercer ce contrôle *a priori*. Si les contre-pouvoirs n'ont pas les moyens de s'exercer, il n'y a plus de garde-fous. En l'état actuel des moyens confiés à l'Arcep, le dispositif présente un risque d'atteinte grave à la liberté d'expression et de communication.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Avis défavorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Vous avez raison : dès lors que de nouvelles prérogatives sont confiées à une autorité, le Gouvernement doit s'assurer qu'elle dispose des moyens nécessaires pour l'exercer. La question est bien identifiée et des discussions sont en cours avec l'Arcep.

Je rappelle qu'avec ces alinéas, qu'il est important de conserver, il s'agit non pas d'organiser une forme de surveillance généralisée des flux sur internet, mais d'autoriser les agents de l'Anssi, après avis conforme de l'Arcep, à placer une balise sur des serveurs suspectés de projeter une attaque contre des autorités publiques, des opérateurs d'importance vitale ou des opérateurs de services essentiels, afin de pouvoir identifier précisément les ressorts de cette attaque. Comme vous le savez, les attaques de ce type peuvent se dérouler sur des périodes de temps relativement longues. J'ajoute que si l'Arcep est en désaccord avec les options retenues par l'Anssi, elle peut se tourner vers le Conseil d'État.

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** Merci pour votre réponse. J'ai bien noté que vous comptiez augmenter les moyens de l'Arcep, ce qui semble nécessaire.

Toutefois, je continue à penser que le dispositif n'est pas satisfaisant : copier l'intégralité de serveurs, même en nombre relativement limité, constitue une atteinte manifeste à la vie privée puisqu'il s'agit de données personnelles. Or, on nous l'a dit cent fois pour nous expliquer qu'il ne fallait pas définir plus précisément la notion de sécurité nationale, l'Anssi ne fait pas du renseignement : c'est une agence qui est placée sous l'autorité du pouvoir exécutif, le Premier ministre en l'occurrence. On voit que la procédure contourne l'autorité judiciaire et que le garde-fou que constitue le contrôle de l'Arcep reste assez limité.

**Mme la présidente.** La parole est à M. Philippe Gosselin.

**M. Philippe Gosselin.** Il est toujours compliqué de placer le curseur au bon endroit. Je relève cependant que le ministre délégué a parlé d'augmenter les moyens de l'Arcep, par ailleurs consacrée en tant qu'autorité administrative indépendante. Que le Gouvernement prenne un engagement ferme sur ce point sera de nature à rassurer les uns et les autres.

**Mme la présidente.** La parole est à M. Loïc Kervran.

**M. Loïc Kervran.** Je tiens à rappeler la spécificité du modèle français, très protecteur car il organise la séparation entre le défensif et l'offensif, entre le civil et le militaire, entre l'Anssi et les services de renseignement. Il diffère en cela des modèles anglo-saxons. Il semble important de dire que, dans le cadre de cette loi de programmation militaire, on ne touche pas à ce qui est une garantie démocratique forte. (*Mme Anne Le Hénauff et M. Jean-Louis Thiériot applaudissent.*)

**M. Philippe Gosselin.** Une vraie singularité !

(*L'amendement n° 1276 n'est pas adopté.*)

**Mme la présidente.** Sur l'amendement n° 1631, je suis saisie par le groupe Renaissance d'une demande de scrutin public.

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

Je suis saisie de deux amendements identiques, n° 1277 et 1614.

La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n° 1277.

**M. Jérémie Iordanoff.** Certes, le renseignement et la sécurité sont séparés dans le modèle français. La difficulté, ici, réside dans le fait qu'on offre des techniques de renseignement à un organisme chargé de la sécurité. Si ce n'était pas le cas, nous n'en serions pas à demander des contrôles plus forts ! Vous devez entendre que, lorsqu'un organisme, placé sous l'autorité du Premier ministre, fait du renseignement, il y a un problème de séparation des pouvoirs.

**M. Ugo Bernalicis.** Vu surtout comment la séparation est respectée en ce moment !

**M. Jérémie Iordanoff.** L'amendement n° 1277, de repli, prévoit que le dispositif est mis en œuvre à titre expérimental et que son évaluation, préalable à sa généralisation, fera l'objet d'un rapport. (*Mme Cyrielle Chatelain et M. Antoine Léaument applaudissent.*)

**Mme la présidente.** La parole est à M. Aurélien Lopez-Liguori, pour soutenir l'amendement n° 1614.

**M. Aurélien Lopez-Liguori.** Après avoir déposé en commission des lois un amendement de suppression de l'article 35, nous revenons en séance dans une démarche constructive. Nous défendons en effet un amendement qui vise à donner un caractère expérimental au dispositif prévoyant d'autoriser l'Anssi, qui dépend, rappelons-le, du secrétariat général de la défense et de la sécurité nationale (SGDSN), lui-même placé sous l'autorité du Premier ministre, à accéder à des données de contenu.

Deux problèmes se posent. Le premier est que vos données de contenu, les miennes, celles de vos familles, seront susceptibles d'être recueillies par des opérateurs pour être transmises à un service gouvernemental, sans contrôle judiciaire préalable. Le second tient au rôle attribué à l'Arcep : l'Auto-

rité sera-t-elle capable de contrôler la mise en place du recueil des données ? La réponse est non. C'est elle-même qui l'affirme dans l'avis qu'elle a formulé sur la loi de programmation militaire en soulignant que « son organisation et son mode de fonctionnement ne lui permettent pas d'assurer une réactivité opérationnelle courte ».

Cette expérimentation permettrait de dresser un premier bilan et de déterminer, avec davantage de visibilité, si la balance entre la protection des libertés et la protection de l'ordre public n'est pas déséquilibrée.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Donner un caractère expérimental au dispositif m'a d'abord paru être une idée très séduisante et j'ai même un temps songé à déposer un amendement similaire. Toutefois, les auditions des différents acteurs concernés m'ont montré que cela risquerait de créer une insécurité juridique, compte tenu des investissements dans les infrastructures qu'un tel projet implique.

Nous serons appelés à voter sur des amendements portant sur l'évaluation des mesures contenues dans les articles 32 à 35, qui nous donneront une meilleure vision de leurs impacts.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Il est toujours séduisant d'expérimenter un dispositif avant de le déployer mais, en l'occurrence, l'évolution des compétences de l'Anssi que nous envisageons est le fruit de l'expérience tirée de la précédente de la loi de programmation militaire. Par ailleurs, ces modifications ont un caractère d'urgence car les Jeux olympiques et paralympiques de 2024 (JOP) provoqueront, selon les experts, un très grand nombre de tentatives d'intrusion – plusieurs dizaines de milliards. Toutes ne porteront évidemment pas atteinte à la sécurité nationale, mais certaines nécessiteront la mise en œuvre des dispositifs que vous aurez adoptés. Il est donc bon que l'Anssi, en lien avec l'Arcep et les acteurs concernés, puisse s'y préparer.

Par ailleurs, le Gouvernement émettra un avis favorable sur l'amendement proposant une évaluation de la mise en œuvre des mesures prévues aux articles 32 à 35, ce qui satisfera à une partie des amendements dont nous discutons. Demande de retrait ou avis défavorable.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** Il est certain qu'à force de couper à la serpe les budgets des autorités administratives indépendantes, on en arrive à de telles situations. L'Arcep n'est du reste pas la seule concernée. Le phénomène est généralisé. La Défenseure des droits, lors de la présentation de son rapport annuel devant la commission des lois, confessait qu'elle n'avait obtenu que 2 des 5 ETPT – équivalents temps plein travaillés – qu'elle demandait, alors même qu'il lui en faudrait 300 à 400 et que ses homologues européens disposent entre cinquante et cent fois plus d'effectifs pour des missions analogues.

Tous ces dispositifs supposent une mise en œuvre par l'exécutif : or je n'ai aucune confiance en lui pour qu'il y procède dans le respect des droits fondamentaux. Aucune ! J'ai été marqué par la lecture d'un récent article de Mediapart retraçant la manière dont un adjudant-chef a pu utiliser à Maignon 300 techniques de renseignement sans suivre le

circuit de validation, passant outre le contrôle censé être exercé par la CNCTR. Qu'est-il arrivé après cela ? Eh bien, il a été promu ! Voilà qui me fait vraiment peur !

Je ne suis pas d'accord pour que l'on confie de telles prérogatives à un gouvernement capable de ne pas respecter les droits fondamentaux et les libertés individuelles.

**M. François Cormier-Bouligeon.** Mais qu'est-ce que vous racontez ?

**M. Ugo Bernalicis.** Les systèmes de garantie dont nous disposerions et dont seraient dépourvus les pays anglo-saxons, c'est du pipeau !

*(Les amendements identiques n<sup>os</sup> 1277 et 1614 ne sont pas adoptés.)*

**Mme la présidente.** La parole est à M. Jérémie Iordanoff, pour soutenir l'amendement n<sup>o</sup> 1278.

**M. Jérémie Iordanoff.** Il importe de circonscrire le champ des données pouvant être collectées par l'Anssi. D'où notre ajout : « Les données collectées 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. » Restons-en au modèle français et ne glissons pas vers le renseignement, sachant que cette collecte relève de l'exécutif. C'est un amendement de bon sens auquel vous serez, je l'espère, favorables.

**Mme la présidente.** Quel est l'avis de la commission ?

**Mme Sabine Thillaye, rapporteure pour avis.** Je tiens à rappeler que l'Anssi n'est pas un service de renseignement et n'a pas vocation à valoriser de telles données. La loi prévoit à cet égard la suppression sans délai des données non pertinentes. En outre, ce sont des agents assermentés et spécialement habilités qui interviendront. La responsabilité pénale pourra donc être engagée. Je suis attachée comme vous aux libertés fondamentales. Simplement, il faudrait parfois arrêter d'être fleur bleue.

**M. Ugo Bernalicis.** Nous nous méfions surtout des agissements du Gouvernement !

**Mme Sabine Thillaye, rapporteure pour avis.** Nous faisons face à des situations critiques et des menaces protéiformes, comme les réunions de la commission de la défense et des forces armées nous le montrent pratiquement chaque semaine. Nous devons trouver un équilibre. On dit parfois que l'Union européenne est un herbivore dans un monde de carnivores. Peut-être ne faudrait-il pas être trop herbivore et tenir un juste milieu ? *(Applaudissements sur les bancs du groupe RE et sur quelques bancs du groupe Dem.)*

**M. Philippe Gosselin.** Très bien !

**M. Ugo Bernalicis.** Nous ne sommes pas fleur bleue avec ce gouvernement. Ceux qui sont fleur bleue, ce sont ceux qui croient à sa bienveillance permanente.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Avis défavorable.

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** Merci pour votre réponse, madame la rapporteure pour avis : vous confirmez que l'Anssi n'a pas besoin de certaines données. Autant qu'elle ne les collecte

pas. Il ne faudrait pas être fleur bleue, d'après vous, mais il n'y a nulle naïveté de notre part. Simplement, nous considérons que, si une copie complète doit être faite, il importe de saisir l'autorité judiciaire. Vous nous renvoyez à l'Europe herbivore. Mais que voulez-vous que nous faisons pour être efficaces ? Que l'on supprime la justice !

**Mme Sabine Thillaye**, *rapporteuse pour avis*. Pas du tout !

**M. Philippe Gosselin**. C'est caricatural !

**M. Jérémie Iordanoff**. Non, ce n'est pas une caricature.

**M. Jocelyn Dessigny**. C'est vous qui êtes une caricature !

**M. Jérémie Iordanoff**. Notre droit prévoit l'intervention de l'autorité judiciaire. Pourquoi vouloir vous affranchir de son contrôle ? Nous voulons des raisons. Nous nous accordons tous sur le fait que le contenu des correspondances n'a pas à faire partie des données collectées. Écrivons-le dans la loi ! C'est simple. (*Mme Sandra Regol applaudit.*)

**Mme la présidente**. La parole est à M. Antoine Léaument.

**M. Antoine Léaument**. Je ne comptais pas intervenir mais vous êtes allée trop loin, madame la rapporteure pour avis. Vous ne pouvez pas nous dire que nous sommes fleur bleue quand il est question de défense des droits. Nous n'avons confiance ni dans ce gouvernement ni dans cette majorité – mot qu'il faudrait mettre entre guillemets puisque vous êtes minoritaires – pour faire respecter d'une manière ou d'une autre la loi, la Constitution ou les principes fondamentaux qui ont présidé à la construction de notre nation. Hier, en commission des affaires sociales, l'opposition s'est vu refuser ses amendements, ce qui est une atteinte majeure au droit d'amender garanti par la Constitution.

**M. François Cormier-Bouligeon**. C'est faux ! Arrêtez avec vos *fake news* !

**M. Antoine Léaument**. Quand un Gouvernement s'en prend aux droits, il est normal de n'avoir aucune confiance en lui. Je vous renvoie à l'article 2 de la Déclaration des droits de l'homme et du citoyen dans lequel est inscrite la résistance à l'oppression. Dès lors qu'il y a oppression, tout citoyen a le droit d'y résister.

**M. François Cormier-Bouligeon**. Quel est le rapport avec cette LPM ?

**M. Antoine Léaument**. Cela a à voir. Quand il est question de la garantie des droits, collègues, vous nous trouverez toujours au travers de votre route. Qu'il s'agisse, dans la LPM, des petits droits, sur lesquels posent question les marqueurs techniques que l'Anssi fournira aux opérateurs, ou des grands !

**M. Mounir Belhamiti**. Mais il y a des garanties !

**M. Antoine Léaument**. Faisons référence à l'article 68 de la Constitution aux termes duquel « nul ne peut être arbitrairement détenu ».

**M. Emeric Salmon** et **M. Jean-Louis Thiériot**. C'est l'article 66 !

**M. Antoine Léaument**. Combien de jeunes gens ont été arbitrairement détenus par votre gouvernement du fait des ordres donnés par M. Darmanin ?

**M. Laurent Jacobelli**. Le problème, c'est que M. Darmanin n'arrête personne !

**M. Philippe Gosselin**. Recentrez-vous sur la LPM !

**M. Antoine Léaument**. Des centaines de jeunes gens ont été arrêtés !

**M. François Cormier-Bouligeon**. Vous vivez dans une réalité parallèle !

**M. Antoine Léaument**. C'est vous qui vivez dans une réalité parallèle ! La manière dont vous avez traité l'opposition à la réforme des retraites, comme la violence que vous avez exercée à l'encontre des citoyens, ne fait que nous renforcer dans notre conviction : nous n'avons pas confiance dans le Gouvernement pour garantir les droits. (*Exclamations sur les bancs des groupes Dem, RE et HOR.*)

### Rappel au règlement

**Mme la présidente**. La parole est à M. Jean-Louis Thiériot, pour un rappel au règlement.

**M. Jean-Louis Thiériot**. Il se fonde sur l'article 54, alinéa 6, auquel je me réfère régulièrement. Je vous propose que l'on revienne à l'ordre du jour qui nous occupe.

Il est savoureux d'entendre le citoyen Léaument nous rappeler l'importance de l'État de droit alors qu'il est un grand défenseur de Robespierre qui, dans ses écrits, se disait opposé à la peine de mort et, dans les faits, a envoyé 17 000 personnes à la guillotine. (*Applaudissements sur les bancs des groupes RE et Dem.*)

**M. Antoine Léaument**. Il faut revoir vos chiffres !

### Article 35 (suite)

**Mme la présidente**. La parole est à M. le ministre délégué.

**M. Jean-Noël Barrot**, *ministre délégué*. Ce rappel au règlement était utile. (*M. Antoine Léaument proteste. – Exclamations sur quelques bancs du groupe RE.*)

**Mme la présidente**. Monsieur Léaument, seul le ministre délégué a la parole.

**M. Jean-Noël Barrot**, *ministre délégué*. Si nous voulons autoriser l'Anssi à collecter des données ciblées, c'est pour éviter que se répètent des cyberattaques comme celle qui a touché, de manière dramatique, l'hôpital de Corbeil-Essonnes, dans le département où se situe votre circonscription, monsieur Léaument, ou celle qu'a subie l'hôpital de Versailles, dans mon propre département. Il se peut que des ennemis de la France, à des fins d'agression, coordonnent de telles attaques afin de compromettre des serveurs et parviennent à les multiplier pour cibler nos institutions publiques, nos OIV et nos OCE, en passant sous les radars de l'Anssi dans l'état actuel des pouvoirs dont elle dispose.

**M. Ugo Bernalicis**. Le problème, ce n'est pas l'objectif, qui peut être louable, c'est de vous donner un blanc-seing !

**M. Jean-Noël Barrot**, *ministre délégué*. Il faut distinguer domaine civil et domaine militaire et rester sur ce qui nous occupe aujourd'hui, la loi de programmation militaire.

(*L'amendement n° 1278 n'est pas adopté.*)

**Mme la présidente.** L'amendement n° 179 de Mme Mélanie Thomin est défendu.

*(L'amendement n° 179, repoussé par la commission et le Gouvernement, n'est pas adopté.)*

**Mme la présidente.** La parole est à Mme Mélanie Thomin, pour soutenir l'amendement n° 180.

**Mme Mélanie Thomin.** Compte tenu du contexte géopolitique que décrivent les chefs d'état-major devant la commission de la défense et des forces armées, je tenais à vous rappeler que personne, dans cet hémicycle, n'avait un comportement de fleur bleue, notamment dans les rangs des oppositions que vous vous plaisez à pointer du doigt, madame la rapporteure pour avis. *(Applaudissements sur les bancs des groupes LFI-NUPES et Écolo-NUPES.)*

Après les tergiversations en commission se pose à nouveau la question de la conservation des données liées à la menace. Pourquoi avoir choisi dix ans pour le délai maximum de conservation ? Madame la rapporteure pour avis, depuis le début de la séance, vos arguments ne nous rassurent pas et nous poussent à nous interroger sur la façon dont vous envisagez l'équilibre entre défense de nos intérêts nationaux et respect de nos libertés fondamentales. En quoi cette durée de dix ans ferait-elle gagner en efficacité ? Méfions-nous de la tendance à allonger les délais de conservation des données. Nous suggérons cinq ans.

*(L'amendement n° 180, accepté par la commission et le Gouvernement, est adopté.)*

**Mme la présidente.** Je mets aux voix l'article 35.

*(Il est procédé au scrutin.)*

**Mme la présidente.** Voici le résultat du scrutin :

Nombre de votants .....	89
Nombre de suffrages exprimés .....	86
Majorité absolue .....	44
Pour l'adoption .....	76
contre .....	10

*(L'article 35, amendé, est adopté.)*

### Article 35 bis

**Mme la présidente.** La parole est à M. Philippe Gosselin.

**M. Philippe Gosselin.** Je souhaite m'exprimer parce que je sais que mon amendement n° 406 rectifié connaîtra un sort funeste si l'amendement de suppression de l'article est adopté.

L'article 35 bis, introduit en commission à l'initiative de notre collègue Philippe Latombe, que je soutenais, oblige les opérateurs d'importance vitale et les opérateurs de service essentiel à cartographier leurs données sensibles et à recourir à un cloud souverain. Bien sûr, je conçois que cela puisse poser quelques difficultés. Toutefois, la protection des données sensibles est un enjeu majeur, tout comme celui du cloud souverain, que nous soulevons à l'environnement depuis des mois, pour ne pas dire des années.

La France accuse, en la matière, de vraies lacunes, même s'il existe des situations pires ailleurs, et nous ne sommes pas au bout de nos peines. Certains considèrent que cet article

arrive trop tôt et qu'il est urgent d'attendre, dans la mesure où il n'y a pas suffisamment d'offres dans ce domaine et que la notion de donnée sensible n'a pas été précisément définie. Peut-être faut-il attendre, en effet. C'est, d'ailleurs, l'objet de l'amendement n° 406 rectifié qui, en repoussant à fin 2024 l'application du présent article, donne un peu de prévisibilité et de visibilité.

Si l'amendement de suppression de l'article 35 bis est adopté, nous devons garder à l'esprit la nécessité de disposer d'un cloud souverain, soit à l'échelle nationale, soit à l'échelle européenne – nous ne pouvons pas, en effet, être nulle part. Enfin, pour le dire de façon un peu triviale, j'ai encore en travers de la gorge, comme d'autres, ce qui s'est passé s'agissant de la plateforme des données de santé, le Health Data Hub (HDH) pour ne pas la citer,...

**M. Ugo Bernalicis.** Ah !

**M. Philippe Gosselin.** ...qui est toujours entre les mains d'une société étrangère bien connue, et dont les données peuvent être récupérées, le cas échéant, en vertu du principe d'extraterritorialité. Disons-le clairement : il n'est pas question de mettre nos industries de défense en difficulté, mais il n'est pas question non plus de laisser nos données sensibles partir je ne sais où ! *(Applaudissements sur quelques bancs du groupe LR. – M. Aurélien Lopez-Liguori applaudit également.)*

**Mme la présidente.** La parole est à M. Aurélien Lopez-Liguori.

**M. Aurélien Lopez-Liguori.** L'article 35 bis part d'un constat dramatique en matière de sécurité et de souveraineté. Il n'est pas rare que les autorités publiques ou des entreprises stratégiques aient recours à des entreprises extra-européennes pour le traitement de leurs données sensibles. L'article prévoit donc que les entités vitales pour notre pays, les OIV et les OSE, ne puissent confier le traitement de ces données qu'à des entreprises françaises ou européennes.

Cette mesure permettra de mettre fin à l'hébergement des données du Health Data Hub par Microsoft, de la direction générale de la sécurité intérieure (DGSI) par Palantir ou encore de Doctolib par Amazon Web Services (AWS). Il est d'ailleurs aberrant que cet article de bon sens ne soit pas d'ores et déjà inscrit dans le droit. Comment les gouvernements successifs ont pu penser un instant que confier à des entreprises étrangères le traitement de données aussi sensibles était une bonne idée, alors que nous disposons désormais d'un écosystème français et européen adapté ? Scaleway ou Docaposte, par exemple, sont en train de créer des solutions de cloud souverain, à même de remplacer AWS ou Microsoft. Comment le Gouvernement a-t-il pu faire preuve d'autant d'irresponsabilité, de naïveté et d'ignorance ? Ou, peut-être, était-ce purement et simplement un choix conscient ? Ce qui serait encore pire.

Signer des contrats avec les entreprises que je viens de citer – AWS, Microsoft ou Palantir –, c'est accepter que les autorités américaines aient accès aux données sensibles des opérateurs vitaux ; c'est vendre les données des Français au plus offrant et bafouer, tout simplement, la souveraineté de notre pays. L'intérêt du présent article est qu'une telle situation ne se reproduise plus. Les banques, les centrales nucléaires, les opérateurs de télécommunications et toutes les entités vitales, qui font que notre pays fonctionne, seront obligés de faire appel aux seules entreprises européennes. Il s'agit d'une mesure de bon sens, qui devrait d'ailleurs être étendue à toute la commande

publique. Les données sont l'or noir du XXI<sup>e</sup> siècle. Nous ne pouvons nous permettre de les confier à des entités extra-européennes, surtout lorsqu'elles sont stratégiques.

**Mme la présidente.** Il faut conclure.

**M. Aurélien Lopez-Liguori.** Pour sécuriser les données de notre pays et écarter tout risque d'ingérence étrangère, nous voterons bien sûr en faveur de l'article 35 *bis*.

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** L'article 35 *bis* a été introduit par voie d'amendement en commission des lois, à mon initiative ; il faisait l'objet d'un sous-amendement visant à temporiser son application en allongeant les délais. Nous examinerons tout à l'heure un amendement de suppression de l'article.

Permettez-moi de faire la distinction, dans mon propos, entre ce que j'en pense à titre personnel et la position du groupe Démocrate (MODEM et indépendants). Je suis bien sûr totalement en phase avec le contenu de l'amendement que j'avais déposé en commission et j'aimerais, monsieur le ministre délégué, que vous nous précisiez les actions que vous comptez engager en la matière. Car si l'amendement de suppression est adopté, nous devons néanmoins pouvoir disposer d'une prévisibilité. Je comprends que des OIV ou des OSE soient amenés à s'interroger quant aux modalités des dispositions qu'il introduit. Mais le problème n'est pas vraiment là. Lorsque l'intérêt national est en jeu, nous ne devons pas faire l'économie de quoi que ce soit mais imposer des règles.

En fonction de ce que vous nous indiquerez, monsieur le ministre délégué, le groupe Dem votera l'amendement de suppression ; à titre personnel, je m'abstiendrai très certainement.

En revanche, il nous faudra aborder le sujet dans les textes à venir, tels que le règlement sur les services numériques (DSA), le règlement sur les marchés numériques (DMA) – qui seront des vecteurs plus appropriés que celui de la LPM que j'avais sous la main – ou, encore, dans le cadre de la transposition de la directive européenne NIS 2, sur laquelle nous devons nous pencher, après d'ailleurs des négociations européennes qui permettront de clarifier le cadre législatif.

**Mme la présidente.** La parole est à Mme Anne Le Héanff.

**Mme Anne Le Héanff.** L'article 35 *bis* résulte de l'adoption de l'amendement de mon collègue Philippe Latombe en commission. J'avais moi-même déposé un amendement identique – que j'ai ensuite retiré –, car il me semblait pertinent, au vu des données sensibles hébergées par les OIV et les OSE, d'obliger ces opérateurs à identifier leurs données sensibles et à prendre des mesures techniques et opérationnelles de nature à protéger ces dernières.

Toutefois, au cours de nos échanges, j'ai compris que le projet de loi de programmation militaire n'était pas le véhicule législatif adapté pour inscrire un tel dispositif, même si nous devons l'instituer rapidement, compte tenu du contexte actuel dans le domaine cyber. Cette nécessité s'inscrit pleinement dans la démarche du Gouvernement et les missions du ministre délégué Jean-Noël Barrot en matière de souveraineté numérique et de protection des données.

C'est pourquoi je souhaite vivement que nous puissions réfléchir de nouveau à ce sujet, monsieur le ministre délégué, dans le cadre d'un grand projet de loi sur le numérique – que

nous avons entamé –, en concertation avec les acteurs de l'écosystème et l'Anssi. Il s'agit pour ces acteurs, comme pour les législateurs qui travaillent sur les sujets du numérique et dont je fais partie, d'une réelle attente depuis des années. C'est aussi la raison pour laquelle je voterai en faveur de l'amendement de suppression de l'article 35 *bis*.

**Mme la présidente.** La parole est à M. Ugo Bernalicis.

**M. Ugo Bernalicis.** L'article que nous avons introduit en commission à l'initiative du collègue Latombe me semblait très bien. Nous étions enfin prêts à reconnaître que la souveraineté numérique et la propriété de nos données devaient entraîner des conséquences opérationnelles et concrètes, ainsi que des garanties pour s'assurer que ce qui s'est produit pour le Health Data Hub ou ce genre de plateformes ne puisse plus se reproduire.

Certains considèrent désormais que ce ne serait pas le bon véhicule législatif. Je rappelle toutefois que, dans les articles 32 à 35, tout ne relève pas exclusivement du domaine militaire : sinon, nous aurions écrit bien moins de choses ! D'ailleurs, ces articles 32 à 35 auraient pu faire l'objet d'une loi spécifique sur le numérique plutôt que de figurer dans la LPM. Votre argument ne tient donc pas vraiment la route, mais admettons. Je comprends qu'il y a dû y avoir un lobbying intense, puisque ces dispositions entraîneraient des conséquences pour certains opérateurs économiques avec lesquels vous entretenez des relations habituelles. C'est sans doute cela qui dérange.

Nous ne voterons donc pas l'amendement de suppression et soutiendrons l'article 35 *bis*, continuant de défendre ainsi le principe selon lequel les données personnelles doivent être détenues de manière souveraine : nous devons avoir la garantie qu'elles ne seront pas utilisées à d'autres fins que celles initialement prévues. Ne soyons pas – comment avez-vous dit, déjà, madame la rapporteure pour avis ? – fleur bleue en la matière.

**M. Jean-Michel Jacques, rapporteur de la commission de la défense nationale et des forces armées.** C'est le bleuet !

**Mme la présidente.** Nous en venons à l'amendement n° 1631, visant à supprimer l'article 35 *bis*. La parole est à M. Mounir Belhamiti.

**M. Mounir Belhamiti.** Je souhaite, pour commencer, féliciter notre collègue Philippe Latombe pour son travail sur la souveraineté numérique, qui dépasse la simple question du cloud souverain, et rappeler que nous partageons largement la nécessité de renforcer la souveraineté de la France dans ce domaine. Toutefois, cet article additionnel arrive trop tôt – je rejoins notre collègue Gosselin sur ce point : preuve en est le grand nombre d'amendements déposés en vue de réécrire l'article qui, en l'état, n'est pas opérant.

**Mme Anne Le Héanff.** Exactement !

**M. Mounir Belhamiti.** Plusieurs arguments permettraient de le démontrer. Cependant, le plus important est de ne pas percuter les négociations en cours au niveau communautaire relatives au schéma européen de certification de cybersécurité pour les services de cloud (EUCS), schéma dont dépend d'ailleurs le référentiel français SecNumCloud, qui est l'un des plus exigeants en la matière. Il est de notre responsabilité de mieux protéger nos données, certes, mais de le faire dans une stratégie globale, avec nos partenaires européens. C'est pourquoi, si je partage, sur le fond, la nécessité d'élargir

l'obligation de recourir à des solutions qualifiées, il me semble important de le faire au bon moment, dans le cadre du véhicule législatif approprié.

Conserver le présent article reviendrait à fragiliser la position française dans ces négociations européennes et affaiblirait la stratégie cloud de confiance et la qualification SecNumCloud qui garantit un haut niveau de protection en matière de cybersécurité, notamment en ce qui concerne les accès illégaux par des États extra-européens aux données les plus sensibles des entreprises et des administrations publiques. C'est pourquoi je propose de supprimer cet article, qui risque d'entraîner comme effet collatéral l'affaiblissement de la position française dans les négociations européennes. (*Applaudissements sur les bancs du groupe RE.*)

**M. Ugo Bernalicis.** C'est faux !

**Mme la présidente.** Quel est l'avis de la commission sur cet amendement de suppression ?

**Mme Sabine Thillaye, rapporteure pour avis.** Nous partageons tous l'objectif de l'article 35 *bis* en matière de souveraineté numérique. Je salue l'engagement de mes collègues Philippe Latombe et Anne Le Hénanff sur ce sujet. Néanmoins, nous devons choisir le bon niveau décisionnel : il se situe actuellement plutôt au niveau de l'Union européenne. Soyons attentifs à ne pas nuire aux négociations en cours sur l'ÉUCS. Je laisse M. le ministre délégué vous apporter une réponse plus précise sur le fond. Avis favorable.

**Mme la présidente.** Quel est l'avis du Gouvernement ?

**M. Jean-Noël Barrot, ministre délégué.** Permettez-moi, à mon tour, de remercier Philippe Latombe de son amendement présenté en commission. Je voudrais dire à la commission et à ses membres que le Gouvernement partage en tout point les objectifs poursuivis. Il est inadmissible que les données sensibles des administrations françaises et des organisations critiques puissent être, en raison de la migration progressive de celles-ci vers le cloud, réquisitionnées par des puissances extra-européennes à des fins d'instruction ou de renseignement.

C'est la raison pour laquelle, il y a quelques années, l'État s'est donné une doctrine, celle du cloud de confiance, et s'est doté d'un référentiel, le SecNumCloud, délivré par l'Anssi, qui permet de garantir qu'une solution d'hébergement en nuage est immunisée contre les réquisitions opérées par des puissances extra-européennes dont la législation a une portée extraterritoriale.

Ceux qui, parmi vous, connaissent bien ces sujets savent que nous ne sommes pas arrivés au bout du chemin. Le 12 septembre dernier, Bruno Le Maire et moi-même avons fait entendre trois messages à Strasbourg.

Premièrement, nous avons affirmé notre volonté de convaincre nos partenaires européens qu'ils devaient se conformer aux mêmes exigences que les nôtres. Depuis, nous avons progressé. Nos avancées éclaireront votre vote sur cet amendement qui vise à supprimer un article adopté en commission – sachant que, jusqu'à présent, le Gouvernement s'était rangé à l'avis de la commission concernant les autres articles. Comme M. Belhamiti l'a expliqué, une discussion très serrée a lieu au niveau européen sur le schéma communautaire de certification du cloud.

**M. Laurent Jacobelli.** Ici, nous parlons de la France, pas de l'Europe !

**M. Jean-Noël Barrot, ministre délégué.** Si, dans son niveau de sécurité le plus élevé, ce schéma retient les mêmes exigences que celles auxquelles nous comptons astreindre nos administrations, voire, ultérieurement, nos organisations critiques – OIV et OSE –, ce sera une grande victoire. En effet, les opérateurs de cloud français et européens qui auront investi pour se conformer à la certification SecNumCloud pourront opérer ailleurs en Europe. Nous aurons aussi la satisfaction de voir l'ensemble des États membres se ranger derrière nos exigences d'immunité face aux législations extraterritoriales. Si, au contraire, nous ne parvenons pas à introduire dans cette certification les mêmes exigences que celles que nous nous sommes imposées, alors, comme souvent lorsque nous devons faire des compromis européens, nous devons revoir à la baisse nos exigences en matière d'immunité.

**M. Laurent Jacobelli.** Comme à chaque fois avec l'Europe !

**M. Jean-Noël Barrot, ministre délégué.** Il est donc indispensable que nous allions au terme des discussions européennes et que nous obtenions gain de cause. Nous avons remporté une première victoire : le 9 mai, la Commission a fait apparaître, pour le critère d'immunité face à l'extraterritorialité dans son projet de certification, le niveau de sécurité le plus élevé. Cependant, la bataille n'est pas terminée. Je me rendrai dès ce soir à Luxembourg pour assister, demain, à un conseil « transports, télécommunications et énergie », en vue de convaincre mes homologues du bien-fondé de cette immunité.

**M. Ugo Bernalicis.** Alors, votons !

**M. Jean-Noël Barrot, ministre délégué.** Si nous adoptons cet article aujourd'hui, certains pays, qui hésitent encore à retenir un niveau de sécurité aussi élevé que le nôtre, s'empresseraient de reprocher à la France d'aller plus vite que la musique et de vouloir imposer trop rapidement des obligations trop contraignantes. Ils s'abrèteraient derrière ces arguments pour faire échouer la négociation.

**M. Bruno Studer.** Bien sûr !

**M. Laurent Jacobelli.** C'est l'Europe qui décide, finalement !

**M. Jocelyn Dessigny.** Quelle soumission !

**M. Jean-Noël Barrot, ministre délégué.** Deuxièmement, Bruno Le Maire et moi-même avons expliqué que ces obligations s'imposeraient aux administrations – c'est un fait. Nous avons ajouté que nous souhaitons que les entreprises privées poussent plus loin la sécurisation de leurs données, et qu'il fallait partir, dans un premier temps, sur une base volontaire. Nous avons ajouté avec beaucoup de gravité que si nos entreprises qui détiennent des données sensibles ne se saisissent pas librement de cette offre de sécurisation, il n'est pas exclu qu'à un moment ou à un autre, nous en venions à une norme obligatoire pour protéger notre souveraineté industrielle et notre indépendance. Je réaffirme cette ambition devant vous. (*MM. Ugo Bernalicis et Thomas Portes s'exclament.*)

**M. Laurent Jacobelli.** Strasbourg n'est pas la capitale de la France !

**Mme la présidente.** Merci de laisser parler M. le ministre délégué, chers collègues.

**M. Jean-Noël Barrot, ministre délégué.** Laissez-moi terminer, c'est important pour éclairer votre vote.

Troisièmement, nous avons annoncé que nous ferions paraître, dans les semaines suivant la réunion, la définition des données sensibles que les administrations françaises devront héberger dans des clouds sécurisés.

**Mme Anne Le Hénauff.** Voilà !

**M. Jean-Noël Barrot, ministre délégué.** Vous avez estimé, monsieur Latombe, que le Gouvernement traînait à publier la révision de la circulaire relative au cloud de confiance, qui définit les données sensibles. J'ai le plaisir de vous annoncer que Mme la Première ministre a signé hier cette circulaire révisée : elle mentionne la définition de ces données dans son neuvième paragraphe. Cela nous permettra d'avancer en aidant les administrations à se préparer à la migration de leurs données sensibles vers un cloud de confiance.

Pour toutes ces raisons, dont les membres de la commission n'avaient peut-être pas connaissance quand ils ont adopté l'article, je vous propose d'adopter cet amendement de suppression. (*Applaudissements sur plusieurs bancs des groupes RE et Dem.*)

**M. Christophe Blanchet.** Très bien !

**Mme la présidente.** La parole est à M. Philippe Latombe.

**M. Philippe Latombe.** J'entends vos explications, monsieur le ministre délégué, et je vous remercie pour la publication de la circulaire, que nous attendions avec impatience depuis Strasbourg. Je souscris par ailleurs aux propos de M. Gosselin : l'État doit montrer l'exemple. À cet égard, nous devons traiter le point noir qu'est la plateforme de données de santé Health Data Hub.

**M. Mounir Belhamiti.** Eh oui !

**M. Philippe Latombe.** Vous pouvez compter sur moi pour vous proposer des solutions dans le cadre du DSA ou du DMA. Nous pourrions même considérer plus largement que les hébergeurs de données de santé doivent rejoindre le référentiel SecNumCloud, ce qui simplifierait le millefeuille administratif de certification.

**M. Mounir Belhamiti.** Tout à fait !

**M. Philippe Latombe.** Je comprends les enjeux politiques européens. Pour avoir discuté avec les opérateurs de certains pays, en particulier hollandais et allemands, je peux témoigner de leur volonté d'aboutir à un consensus et de mener une négociation équilibrée, dont la France ne prendrait pas les rênes et dans laquelle elle n'imposerait pas ses vues. J'entends cet argument. C'est une des raisons pour lesquelles le groupe Dem votera la suppression de l'article 35 *bis*.

Le présent débat se posera à nouveau lors de la transposition de la directive NIS 2. Comptez donc sur moi pour soumettre une nouvelle fois l'article 35 *bis*, sous réserve des résultats de la négociation européenne. J'espère sincèrement que vous convaincrez vos homologues que le schéma européen de certification de cybersécurité pour les services de cloud doit intégrer la clause d'immunité. Ce problème n'est pas franco-français, il est bel et bien européen : l'Union européenne doit absolument comprendre que l'extraterritorialité américaine ou chinoise est un sujet de préoccupation. Si nous n'aboutissons pas à un accord, nous devons étudier la façon dont le droit national peut nous prémunir contre ce risque. C'est important pour nos entreprises et pour l'ensemble de nos concitoyens.

**M. Mounir Belhamiti.** Il a raison !

**Mme la présidente.** La parole est à Mme Mélanie Thomin.

**Mme Mélanie Thomin.** Les députés du groupe Socialistes et apparentés ne suivront pas le renoncement de la majorité présidentielle, qui témoigne, à nos yeux, de vos tergiversations avec le monde économique. (*Applaudissements sur plusieurs bancs du groupe Écolo-NUPES. – M. Thomas Portes applaudit également.*) Vous évoquez un effet contre-productif dans votre exposé sommaire, et vous observez que les contraintes légales ne conviennent pas aux entreprises : il n'en faut pas plus pour que vous décidiez de les retirer au beau milieu de la partie. C'est un renoncement pour notre autorité politique. Qui décide en matière de sécurité et de protection des libertés ? Votre renoncement exacerbe nos inquiétudes quant à la préservation de l'État de droit. Vous avez pour credo de laisser faire le marché mais, dans le contexte actuel, où les guerres d'influence n'épargnent pas le monde économique, il est dangereux de se laisser guider par une telle priorité. Monsieur le ministre délégué, êtes-vous dans l'hémicycle pour défendre le monde de l'entreprise ou pour faire valoir notre défense ?

**M. Antoine Léaument.** Bien vu !

**Mme Mélanie Thomin.** Vos propos révèlent combien la puissance de l'économie et des entreprises pèse dans nos débats. Nous y sommes bien évidemment opposés.

**M. Antoine Léaument.** Très bien !

**M. Laurent Jacobelli.** Il faut reconnaître qu'elle a raison !

**Mme la présidente.** La parole est à M. Aurélien Lopez-Liguori.

**M. Aurélien Lopez-Liguori.** J'ai bien écouté vos arguments, monsieur le ministre délégué et monsieur Belhamiti. Toutefois, nous n'avons aucune confiance dans l'Union européenne s'agissant du numérique souverain. Chacun se souvient du projet de cloud européen Gaia-X : il devait être souverain mais, en définitive, Alibaba et AWS y participent.

Vous estimez que le vote de l'article 35 *bis* affaiblirait la capacité de la France à mener des négociations européennes. Pourtant, Bruno Le Maire n'a pas attendu l'Union européenne pour proposer à l'Assemblée de voter la taxe Gafa. Ce faisant, a-t-il affaibli la capacité de négociation de la France ? Je ne le crois pas. Prendre un peu d'avance nous permet d'entraîner l'Union européenne dans notre sillage. M. Belhamiti craignait qu'il ne soit trop tôt pour avancer en ce sens ; au contraire, il est peut-être trop tard, vu l'engouement que suscite l'intelligence artificielle, technologie qui repose sur l'accumulation de données et l'apprentissage automatique.

**M. Erwan Balanant.** Pas tout à fait !

**M. Aurélien Lopez-Liguori.** Alors que l'article 35 *bis* nous offre la possibilité de relocaliser nos données en Europe et en France, pour créer les géants du numérique européens et français que nous appelons tous de nos vœux, vous proposez de le supprimer. C'est regrettable. Vos arguments ne tiennent pas. C'est pourquoi nous ne voterons pas l'amendement de suppression de l'article 35 *bis*. (*Applaudissements sur plusieurs bancs du groupe RN.*)

**Mme la présidente.** La parole est à M. Bruno Studer.

**M. Bruno Studer.** Permettez-moi un petit rappel d'histoire parlementaire – il sera utile à ceux qui voudront bien l'entendre. Pour illustrer l'enjeu de la chronologie nationale

et européenne, je vous renvoie au vote de la directive sur le droit d'auteur, qui était en concurrence, dans le calendrier, avec la proposition de loi tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse. Certains pays avaient adopté une législation sur les droits voisins à l'échelle nationale, avant que l'Union ne décide de légiférer sur le sujet. Nous avons nous-mêmes été tentés de le faire, mais le Gouvernement avait préféré temporiser. En définitive, la France a arraché au Parlement européen la directive sur le droit d'auteur en mai 2019 ; elle fut le premier État membre à la transposer en juillet 2019, donnant l'exemple et suscitant une impulsion. Le fait d'avoir temporisé et d'avoir joué un jeu collectif a été bénéfique – je suis toutefois conscient que certains, parmi vous, ne souhaitent pas jouer collectif sur le terrain européen.

**M. Laurent Jacobelli.** On ne joue pas collectif sur le terrain de la souveraineté !

**M. Bruno Studer.** Vous opposez systématiquement ces deux dimensions – c'est votre droit. Je le répète, l'histoire parlementaire nous apprend qu'au sujet des droits voisins, nous avons attendu que la directive sur le droit d'auteur aboutisse et l'avons ensuite transposée en quelques semaines. Nous avons été à la manœuvre, non pas en faisant cavalier seul, mais en jouant collectif – avec l'intervention active de notre collègue Patrick Mignola. (*Applaudissements sur plusieurs bancs des groupes RE et Dem.*)

**M. Christophe Blanchet.** Enfin un peu de hauteur !

**M. Aurélien Lopez-Liguori et M. Ugo Bernalicis.** Et la taxe Gafa ?

**Mme la présidente.** La parole est à M. Antoine Léaument.

**M. Antoine Léaument.** Je ne comprends pas vos arguments – ou plus exactement, ils m'inquiètent. Vous expliquez que nous ne pouvons pas voter l'article 35 *bis* car cela nous affaiblirait dans la négociation européenne. N'importe quoi ! C'est l'inverse.

**M. Ugo Bernalicis.** Eh oui !

**M. Antoine Léaument.** Si le Parlement français décide d'adopter des mesures plus restrictives que celles que prévoit l'Union, vous pourrez vous en prévaloir dans la négociation européenne. (*Applaudissements sur plusieurs bancs du groupe LFI-NUPES.*) Nous renforçons notre pays en prenant de telles décisions.

**M. Erwan Balanant.** Il n'a pas suivi ! On vient pourtant de lui expliquer le contraire !

**M. Antoine Léaument.** Nous défendons précisément l'intérêt national en refusant de voter votre amendement de suppression de l'article 35 *bis*. Vous expliquez tout à la fois que le dispositif prévu par l'article est génial, qu'il faut remercier M. Latombe pour son travail, mais qu'il faut le supprimer : vous rendez-vous compte de l'absurdité de l'argument ? D'après vous, le dispositif ne serait pas placé au bon endroit ; ce serait un cavalier législatif.

**M. Mathieu Lefèvre.** Vous devriez écouter M. Studer !

**M. Antoine Léaument.** Nous sommes pourtant bien en train de modifier le code de la défense, et nous examinons la loi de programmation militaire. Je vois davantage de rapport entre cet article et la défense que, par exemple,

entre les mesures de surveillance générale et la loi relative aux Jeux olympiques et paralympiques dans laquelle vous les avez introduites : voilà un vrai cavalier législatif.

Enfin, c'est vous qui êtes fleur bleue. Êtes-vous conscients que des nations de l'Union européenne pourraient nous espionner ? L'Allemagne n'a-t-elle pas espionné la France, comme nous l'avons appris en 2015 ? L'article 35 *bis* rappelle que « la captation par une puissance étrangère ou par une organisation étrangère ou sous contrôle étranger porterait une possible atteinte aux intérêts fondamentaux de la nation ». Notre rôle est précisément de défendre les intérêts de la nation, et non de mener des discussions européennes. (*Applaudissements sur plusieurs bancs des groupes LFI-NUPES et Écolo-NUPES.*)

**Mme la présidente.** La parole est à M. Jérémie Iordanoff.

**M. Jérémie Iordanoff.** Les députés du groupe Écologiste-NUPES estiment que, de façon générale, l'Europe est un échelon de souveraineté pertinent pour les données. Cela n'empêche pas que les données très sensibles, touchant à la sécurité nationale, restent traitées à l'échelon national. De fait, nous ne comprenons pas l'argument selon lequel il faudrait attendre une législation européenne, qui sera peut-être plus souple que celle de la France et qui nous obligera à nous aligner vers le bas.

**M. Jean-Noël Barrot, ministre délégué.** Nous n'aurons pas le choix !

**M. Jérémie Iordanoff.** Pourquoi le législateur français n'adopterait-il pas une législation stricte ? Qu'est-ce qui nous interdit de dépasser la norme européenne en matière de protection des données et d'être mieux-disants ? (*Applaudissements sur plusieurs bancs des groupes Écolo-NUPES et LFI-NUPES.*) La loi de programmation militaire concerne la défense nationale, non la défense européenne, qui relève du Parlement européen.

**Mme la présidente.** La parole est à M. le ministre délégué.

**M. Jean-Noël Barrot, ministre délégué.** Madame Thomin, je n'ai que faire de l'intérêt des actionnaires des grands groupes, en l'occurrence des OIV et des OSE.

**M. Jocelyn Dessigny.** Ah, j'ai eu peur !

**M. Jean-Noël Barrot, ministre délégué.** Il s'agit ici de la souveraineté nationale et de la protection des données personnelles ou sensibles.

**M. Laurent Jacobelli.** Il s'agit de la souveraineté nationale, mais vous parlez d'Europe !

**M. Jean-Noël Barrot, ministre délégué.** Je trouve un peu dommage de terminer la discussion de ces articles par de telles allégations.

Monsieur Léaument, je vous invite à participer aux discussions avec nos partenaires européens.

**M. Antoine Léaument.** C'est vrai ? Si vous m'invitez, je viens !

**M. Jean-Noël Barrot, ministre délégué.** Vous affirmez que nos arguments sont absurdes, mais commencez donc par les écouter : vous pourrez ensuite en juger. Si les autres pays font preuve d'étonnement, voire de suspicion envers la position française en la matière, c'est précisément parce que la France a avancé plus vite et plus loin que les autres.

**M. Bruno Studer.** Bien sûr !

**M. Jocelyn Dessigny.** Vous vous êtes trompé de parlement, monsieur le ministre délégué ! Nous sommes ici à l'Assemblée nationale, pas au Parlement européen !

**M. Jean-Noël Barrot, ministre délégué.** Nous souhaitons que le niveau de sécurité le plus élevé du schéma de certification en cours de discussion reflète les exigences auxquelles nous voulons astreindre nos administrations et, à terme, nos entreprises. Si les négociations aboutissent à cela, c'est tant mieux ; sinon, c'est un drame, car nous n'aurons pas d'autre choix que d'adopter un référentiel conforme au référentiel européen.

**M. Bruno Studer.** Exactement !

**M. Ugo Bernalicis.** Non, il s'agit d'un domaine régalien.

**M. Jean-Noël Barrot, ministre délégué.** Les exigences que nous avons pour nos administrations, nos OIV et nos OSE, décrites dans cet article, seront alors hors d'atteinte, car le choix européen sera moins strict que celui que nous aurions souhaité. (*Applaudissements sur plusieurs bancs du groupe RE.*)

**M. Laurent Jacobelli.** Votre argument ne tient pas la route une seconde !

**M. Jean-Noël Barrot, ministre délégué.** Monsieur Lopez-Liguori, vous avez raison au sujet de la taxe Gafa, mais la situation n'est pas comparable. Il s'agissait alors d'une négociation internationale menée sous l'égide de l'Organisation de coopération et de développement économiques (OCDE), lors de laquelle nous tâchions de faire plier les États-Unis.

**M. Bruno Studer.** Bien sûr !

**M. Jean-Noël Barrot, ministre délégué.** Dans le cas qui nous occupe actuellement, si nous perdons la bataille de la certification européenne, alors nous perdrons tout. C'est la raison pour laquelle nous ne devons pas, à ce stade, donner des arguments aux lobbyistes des géants du numérique...

**M. Laurent Jacobelli.** Oh !

**M. Jean-Noël Barrot, ministre délégué.** ...qui abreuvent certains pays européens dans l'espoir de faire obstacle à l'instauration d'une telle certification. (*Applaudissements sur plusieurs bancs du groupe RE.*)

**Mme la présidente.** Je mets aux voix l'amendement n° 1631.

(*Il est procédé au scrutin.*)

**Mme la présidente.** Voici le résultat du scrutin :

Nombre de votants .....	97
Nombre de suffrages exprimés .....	96
Majorité absolue .....	49
Pour l'adoption .....	67
contre .....	29

(*L'amendement n° 1631 est adopté ; en conséquence, l'article est supprimé.*)

**Mme la présidente.** La suite de la discussion est renvoyée à la prochaine séance.

2

#### ORDRE DU JOUR DE LA PROCHAINE SÉANCE

**Mme la présidente.** Prochaine séance, cet après-midi, à quinze heures :

Suite de la discussion du projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.

La séance est levée.

(*La séance est levée à treize heures cinq.*)

*Le directeur des comptes rendus*

Serge Ezdra