ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Compte rendu

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

Mercredi
10 mai 2023
Séance de 14 heures 30

Compte rendu n° 54

SESSION ORDINAIRE DE 2022-2023

Présidence de M. Sacha Houlié, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 14 heures 35.

Présidence de M. Sacha Houlié, président,

La Commission poursuit l'examen des articles 32 à 35, délégués au fond par la commission de la défense et des forces armées, du projet de loi relatif à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (n° 1033) (Mme Sabine Thillaye, rapporteure pour avis).

M. le président Sacha Houlié. Nous reprenons nos travaux à l'article 34.

Article 34 *(Art. L.* 2321-4 [nouveau] du code de la défense) : Obligation d'information de l'ANSSI et des utilisateurs par les éditeurs de logiciel en cas de vulnérabilité significative ou d'incident informatique.

Amendements CL31 de Mme Anne Le Hénanff et CL99 de Mme Sabine Thillaye (discussion commune).

Mme Anne Le Hénanff (HOR). Le périmètre de l'article est très large puisqu'il prévoit d'obliger les éditeurs à notifier toute faille de sécurité dont ils auraient connaissance. S'il semble indispensable qu'ils signalent systématiquement et dans les plus brefs délais à l'Agence nationale de la sécurité des systèmes d'information (Anssi) les vulnérabilités et les incidents susceptibles de porter atteinte à la sécurité nationale, cette obligation serait disproportionnée si elle s'appliquait à toutes les failles éventuelles.

Il vous est, par conséquent, proposé de préciser que la vulnérabilité, en plus d'être significative, doit être susceptible de porter atteinte à la sécurité nationale.

Mme Sabine Thillaye, rapporteure pour avis. Afin de clarifier le texte et de rendre le dispositif plus intelligible, l'amendement CL99 vise à préciser que les incidents et les vulnérabilités visés doivent être significatifs.

Je suis sensible à la volonté des auteurs de l'amendement CL31 de préciser et d'encadrer l'article, néanmoins, je les invite à retirer cet amendement au profit du mien. Les éditeurs, s'ils ont la responsabilité de déclarer les vulnérabilités de leurs logiciels, ne sont pas habilités à apprécier l'atteinte à la sécurité nationale, qui est une prérogative de l'État.

M. Philippe Latombe (Dem). La question se pose en effet de savoir qui est à même de considérer que la sécurité nationale est en jeu, d'autant plus que de nombreux logiciels sont revendus par les éditeurs qui les ont conçus à d'autres éditeurs, qui les intègrent ensuite dans leurs propres solutions.

Il semble préférable de retenir l'amendement de Mme la rapporteure pour avis, même s'il conviendrait de le retravailler avant l'examen en séance publique afin d'intégrer la notion de sécurité nationale. C'est l'objectif que nous visions pour ces articles du titre V dans lequel la sécurité nationale semble avoir été oubliée alors qu'il a trait à la sécurité des systèmes d'information.

M. Ugo Bernalicis (LFI-NUPES). Si j'ai bien compris, nous voudrions que les éditeurs de logiciel préviennent l'Anssi de toute faille dans la sécurité ou de toute vulnérabilité de leurs logiciels, car il se trouve que l'État et les administrations utilisent ces

mêmes logiciels et que les défaillances de ces derniers pourraient provoquer des dégâts autrement plus graves que chez de simples particuliers.

Or vous venez de dire, madame la rapporteure pour avis, que les éditeurs de logiciel ne sont pas à même de juger si leurs produits risquent de porter ou non atteinte à la sécurité nationale. C'est d'autant plus vrai qu'une faille bénigne pour eux pourrait se révéler catastrophique pour l'État, en offrant un point d'entrée pour des systèmes visant à compromettre des données. L'esprit du texte, me semble-t-il, est d'exiger des éditeurs qu'ils signalent toutes les vulnérabilités, toutes les failles, sans chercher à les hiérarchiser, cette tâche incombant à l'Anssi qui évaluera si ces difficultés présentent un risque pour nos services. Or, si vous prévoyez que les éditeurs n'auront à transmettre que les failles ou les vulnérabilités significatives, vous faites reposer sur leurs épaules la charge de décider ce qui est significatif ou non. Est-ce là ce que nous voulons ? Pour toutes ces raisons, je ne voterai pas l'amendement de la rapporteure pour avis.

L'amendement CL31 est ***retiré****.*

La commission ***adopte*** *l'amendement CL99.*

Amendement CL39 de M. Philippe Latombe.

M. Philippe Latombe (Dem). L'amendement tend à limiter l'obligation d'information qui pèse sur les éditeurs de logiciel aux seuls clients professionnels. Le code de la consommation a prévu d'autres dispositions pour informer les autres consommateurs. L'Anssi peut communiquer des informations, la Commission nationale de l'informatique et des libertés (Cnil) a l'obligation d'informer les clients en cas de fuite de données personnelles.

Si les logiciels sont revendus à d'autres éditeurs qui les intègrent dans leurs propres solutions et que des failles apparaissent, les clients professionnels, hôpital ou collectivité par exemple, seront tout de même informés. Notre proposition limite le champ des consommateurs informés mais pas la portée. L'Anssi y serait favorable.

Mme Sabine Thillaye, rapporteure pour avis. Je comprends le sens de votre amendement et partage votre objectif mais la rédaction n'est pas sécurisante, car les logiciels à caractère grand public peuvent être utilisés par des professionnels, ce que votre amendement ne prend pas en compte.

Je vous invite à retirer votre amendement au bénéfice de celui que je vous présenterai dans quelques instants, le CL100, qui a pour objet de limiter l'obligation d'information aux seuls utilisateurs professionnels, que vous visez d'ailleurs dans votre exposé sommaire.

Par ailleurs, un travail de rédaction sur une définition des éditeurs de logiciel est en cours. J'espère qu'il aboutira d'ici à l'examen en séance publique.

M. Philippe Latombe (Dem). J'accepte de le retirer mais votre rédaction ne permet pas de s'assurer que l'ensemble des logiciels soient concernés. Vous visez, vous aussi, les utilisateurs professionnels, mais des logiciels pourraient passer entre les mailles du filet.

M. Ugo Bernalicis (LFI-NUPES). Je pense qu'au contraire, il ne faudrait pas préciser. Tous les utilisateurs, qu'ils soient des professionnels ou non, devraient être informés. Certes, d'autres dispositions prévoient déjà l'obligation d'avertir les particuliers mais mieux

vaut prévoir large et n'oublier personne plutôt que d'en omettre certains à force de restreindre le champ des personnes à informer. L'usage professionnel n'est pas clairement défini et je me demande quel sort vous comptez réserver à ceux qui sont des professionnels mais qui ne se sont pas déclarés en tant que tels lorsqu'ils ont téléchargé un logiciel, par exemple parce qu'il serait libre de droits.

L'amendement est ***retiré****.*

Amendement CL26 de M. Ugo Bernalicis.

M. Ugo Bernalicis (LFI-NUPES). Je ne crois pas en l'altruisme des éditeurs de logiciel, car ils ont une réputation à préserver. Il est arrivé à de nombreuses reprises que des failles informatiques importantes soient révélées à la suite de fuites émanant des personnels de ces sociétés. Les sociétés n'en ont pas informé leurs clients alors qu'elles en avaient l'obligation. C'est pourquoi je vous propose de sanctionner les éditeurs de logiciel en cas de manquement à leurs obligations par une amende administrative pouvant atteindre 4 % de leur chiffre d'affaires.

Mme Sabine Thillaye, rapporteure pour avis. À ce stade, l'introduction de sanctions n'est pas souhaitable, le dispositif prévoyant déjà de publier les vulnérabilités en cas de non-respect de l'injonction de l'Anssi. C'est le fameux *name and shame.*

Je reste attentive à l'équilibre des dispositions votées et aux charges qui pèsent sur les personnes et les structures concernées.

Pour être honnête avec vous, sachez que je me suis renseignée sur la pertinence de prévoir ou non des sanctions et, après avoir auditionné les acteurs concernés, il me semble préférable d'en rester là, quitte à envisager une évolution ultérieure du dispositif si le *name and shame* ne suffisait pas.

M. Ugo Bernalicis (LFI-NUPES). Le juge peut choisir d'infliger ou non une sanction administrative. Le *name and shame* ne suffit pas. Encore récemment, de grandes entreprises ont refusé de révéler des fuites de données. Peut-être auront-elles été en difficulté quelques mois durant lesquels leur cotation en bourse aura reculé, mais elles existent encore et leur chiffre d'affaires n'en a pas souffert. Les gens ne sont pas à l'affût de ce type d'information et ne passent pas leur temps à lire la presse spécialisée. La plupart d'entre eux ne sauront pas que leurs données ont été mises en ligne, piratées par des hackers et revendues si l'obligation d'information qui pèse sur l'éditeur de logiciel n'est pas sanctionnée par une amende et que l'État n'en contrôle pas le respect.

Ne soyons pas naïfs ! Un rapport de force est engagé avec les éditeurs de logiciel, qui profitent parfois du monopole qu'ils détiennent sur le marché pour asseoir leur toute-puissance. C'est un problème dont nous avons déjà discuté, notamment à propos des techniques de renseignement pour lesquelles il n'existe qu'un ou deux logiciels sur le marché, ce qui vide de sa substance le *name and shame* ! Quoi qu'il arrive, vous dépendez d'eux ! Frapper au portefeuille d'une personne morale à but lucratif me semble un bon moyen de la dissuader.

La commission ***rejette*** *l'amendement.*

Amendements CL1 de M. Sébastien Chenu et CL49 de M. Mounir Belhamiti (discussion commune).

Mme Marie-France Lorho (RN). L'amendement CL1 tend à clarifier le délai auquel sont soumis les éditeurs de logiciel pour informer les utilisateurs d'une vulnérabilité significative ou d'un incident informatique de nature à compromettre la sécurité de leurs systèmes d'information et d'affecter un de leurs produits. Si une telle vulnérabilité ou un tel incident est détecté par l'éditeur de logiciel, celui-ci doit impérativement en informer ses utilisateurs afin de leur permettre de prendre les dispositions qui s'imposent. Au regard des enjeux de cybersécurité, cette information doit être transmise dans un délai maximal de soixante-douze heures à compter de la découverte de la vulnérabilité ou de l'incident.

Mme Sarah Tanzilli (RE). L'amendement CL49 vise à prévoir le délai dans lequel les éditeurs de logiciel informent leurs utilisateurs de la vulnérabilité significative qui affecte un de leurs produits ou d'un incident informatique qui compromettrait la sécurité de leurs systèmes d'information et pourrait affecter l'un de leurs produits. Nous proposons que ce délai soit fixé par l'Anssi pour assurer une meilleure réactivité face à la menace et éviter de potentiels abus.

Mme Sabine Thillaye, rapporteure pour avis. En la matière, la disposition étant déjà suffisamment contraignante pour les éditeurs, il serait souhaitable de laisser un peu de flexibilité et de ne pas prévoir de délais trop contraints.

Je suis néanmoins d'accord avec vous sur un point : il faut préciser au maximum le dispositif. C'est pourquoi je préfère l'amendement CL49, qui laisserait le soin de déterminer le délai à l'Anssi, laquelle pourra apprécier la situation *in concreto*, et prendre une décision adaptée à l'ampleur de l'incident et de la vulnérabilité.

Successivement, la commission ***rejette*** *l'amendement CL1 et* ***adopte*** *l'amendement CL49.*

Amendement CL25 de M. Ugo Bernalicis.

M. Ugo Bernalicis (LFI-NUPES). Nous voulons transformer en obligation la possibilité que ce texte se contente d'offrir à l'Anssi d'enjoindre aux éditeurs de logiciel d'informer leurs utilisateurs en cas de vulnérabilité ou d'incident affectant leur produit. Je ne comprends pas que vous ne soyez pas plus contraignants. Tenez-vous tant que cela à vous montrer sympathiques avec ces éditeurs et à ne pas trop les brusquer au prétexte que vous dépendez d'eux ? Si c'est vraiment l'explication, il devient urgent de nous doter des moyens de développer nos propres solutions informatiques.

Mme Sabine Thillaye, rapporteure pour avis. Le dispositif juridique doit rester souple et proportionné. Imposer une publication rigidifierait excessivement le texte. L'Anssi doit conserver son libre arbitre et apprécier, au regard de l'ampleur de la vulnérabilité ou de l'incident, la nécessité de prendre une telle décision. Tous les jours, des incidents informatiques se produisent.

M. Ugo Bernalicis (LFI-NUPES). Le texte prévoit qu'en cas de vulnérabilité significative – cet adjectif ayant été ajouté par vos soins, madame la rapporteure pour avis –, les éditeurs de logiciel doivent en informer les utilisateurs. S'ils ne le font pas, vous considérez qu'il serait suffisant de proposer à l'Anssi de leur demander de le faire. Mais dès lors que vous prévoyez, dans ce texte, que les éditeurs doivent informer leurs utilisateurs dans certains cas, vous devez, en cas de manquement de leur part, en tirer des conclusions et prendre les mesures qui s'imposent ! Vous ne pouvez pas vous dédire deux alinéas plus loin.

À moins qu'il ne s'agisse que d'une obligation de façade et que vous vous laissiez toute latitude pour négocier. Finalement, celui dont les données auront été pillées se retrouve soumis à l'arbitraire d'un rapport de force entre l'Anssi et les éditeurs de logiciel. Ce n'est pas normal.

M. Philippe Latombe (Dem). Je me suis, moi aussi, demandé s'il fallait imposer une injonction et j'en ai discuté avec les éditeurs, l'Anssi et d'autres acteurs concernés. Le problème est que, tant qu'un patch n'a pas été trouvé pour corriger la faille, la publication de l'événement pourrait inciter les hackers à s'engouffrer dans la brèche. Il faut laisser à l'Anssi la latitude de décider du moment le plus opportun pour informer.

M. Ugo Bernalicis (LFI-NUPES). Mais il est indiqué que l'information doit être transmise « dans les meilleurs délais » ! On ne demande pas l'immédiateté !

M. Philippe Latombe (Dem). Certes, mais il arrive que les logiciels soient intégrés dans d'autres et qu'il faille du temps avant de corriger la vulnérabilité. La rendre publique serait dangereux.

*La commission **rejette** l'amendement.*

Amendement CL68 de M. Aurélien Lopez-Liguori.

M. Jordan Guitton (RN). L'article 34 prévoit un dispositif de remontée des vulnérabilités significatives et des incidents informatiques des éditeurs de logiciel à l'Anssi. L'agence aurait ainsi la possibilité de publier ces informations si l'entreprise n'a pas mis les utilisateurs au courant, même si la vulnérabilité n'a pas été réparée. La méthode est étonnante et s'apparente à une forme de chantage déguisé. Ce sont des procédés de hacker ! Vous autorisez l'Anssi à divulguer des données compromettantes pour faire plier sa cible. Comment justifier une telle doctrine ? Comment expliquer que l'on donne à une agence, qui dépend du Gouvernement, le pouvoir d'exposer des entreprises à des attaques de hackers ? Cette épée de Damoclès qui pèserait sur la tête des entreprises récalcitrantes ne peut pas être le moyen d'obliger les entreprises à remédier aux incidents et aux vulnérabilités.

Si une entreprise dont les failles ont été publiées par l'Anssi est attaquée, qui sera responsable ? L'entreprise ou l'Anssi ? Contre qui la victime se retournera-t-elle pour demander réparation ? Quand une mesure soulève plus de questions qu'elle n'en règle, c'est qu'elle doit être réécrite. Nous vous proposons, par conséquent, que l'Anssi ne puisse procéder à cette publication tant que l'éditeur de logiciel n'a pas remédié à la vulnérabilité ou à l'incident.

Mme Sabine Thillaye, rapporteure pour avis. Nous venons précisément d'en discuter : laissons l'Anssi décider des modalités de publication et d'information. Avis défavorable.

M. Jordan Guitton (RN). Le problème est que l'Anssi n'est pas indépendante du Gouvernement.

M. Philippe Latombe (Dem). Votre question rejoint la discussion que nous avons eue au précédent amendement. Si nous adoptons le vôtre, l'Anssi ne pourra agir tant que la vulnérabilité n'a pas été réparée. Dans un souci d'équilibre, il faudrait aussi prévoir que l'Anssi puisse enjoindre à l'entreprise de réparer la vulnérabilité. Sinon, il suffirait que l'éditeur ne fasse rien pour que l'incident ne soit jamais publié.

*La commission **rejette** l'amendement.*

Amendement CL100 de Mme Sabine Thillaye.

Mme Sabine Thillaye, rapporteure pour avis. L'amendement tend à ce que seuls les utilisateurs professionnels soient informés en cas de vulnérabilité des produits, pour alléger la charge que fait peser cette disposition sur les éditeurs, sans méconnaître pour autant la portée ni l'objectif de l'article.

*La commission **adopte** l'amendement.*

Amendement CL32 de Mme Anne Le Hénanff.

Mme Anne Le Hénanff (HOR). Si certaines dispositions législatives actuelles s'appliquent aux éditeurs de logiciel, ces derniers n'y sont pas expressément définis. Dans un souci de clarté, il conviendrait de définir la notion d'éditeur de logiciel.

Ainsi, nul ne pourra prétendre se soustraire aux dispositions de l'article dès lors que son activité correspondra à la définition que nous vous proposons, dans la continuité de la jurisprudence rendue en la matière : « Toute personne assurant la conception, le développement, l'exploitation et la commercialisation de produits logiciels est un éditeur de logiciel ».

Mme Sabine Thillaye, rapporteure pour avis. Je suis favorable à tout amendement qui pourrait éclaircir la loi et je soutiens le principe de l'ajout d'une telle définition. Cependant, la rédaction que vous proposez exclurait les éditeurs de logiciel libre, ce qui fragiliserait le dispositif juridique. Je vous invite à retirer l'amendement afin de le retravailler avant l'examen en séance publique.

*L'amendement est **retiré**.*

*Suivant la préconisation de la rapporteure pour avis, la commission **rejette** l'amendement CL11 de Mme Mélanie Thomin.*

Amendement CL95 de Mme Sabine Thillaye.

Mme Sabine Thillaye, rapporteure pour avis. L'amendement tend à préciser la portée de l'article 34 en y intégrant la définition de l'incident informatique telle qu'elle est formulée dans la directive NIS 2 (Network and information security), cette définition n'existant pas encore en droit français.

*La commission **adopte** l'amendement.*

Amendement CL27 de M. Ugo Bernalicis.

M. Ugo Bernalicis (LFI-NUPES). Il serait bon que le décret qui sera pris en Conseil d'État pour préciser les dispositions de l'article 34 ne le soit qu'après avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). L'intégrité de l'Anssi dépend de la capacité de contrôle de l'Arcep.

Mme Sabine Thillaye, rapporteure pour avis. Je ne suis pas défavorable à l'amendement mais l'article 34, qui prévoit d'alerter l'Anssi et les utilisateurs de logiciels en

cas de vulnérabilité et d'incident informatique significatifs, n'entre pas dans le périmètre de l'Arcep, qui est le régulateur des communications électroniques. Cet ajout ne me semble donc pas fondé en droit et il n'a pas été demandé par l'Arcep. Avis favorable néanmoins.

*La commission **adopte** l'amendement.*

Amendements CL33 de Mme Anne Le Hénanff et CL98 de Mme Sabine Thillaye (discussion commune).

Mme Anne Le Hénanff (HOR). Il s'agit d'un amendement de repli. Nous proposons que le décret d'application précise « le type de vulnérabilité et d'incident informatique que les éditeurs de logiciel sont tenus de signaler à l'Anssi ».

Mme Sabine Thillaye, rapporteure pour avis. Comme vous, je propose que le décret en conseil d'État précise les critères d'appréciation du caractère significatif de la vulnérabilité ou de l'incident. Mais j'ajoute que ces critères se fonderont sur des pratiques et standards internationaux communément admis, comme le système d'évaluation des vulnérabilités, le CVSS, qui fait référence en la matière. Je vous invite donc à retirer votre amendement au profit du mien.

M. Philippe Latombe (Dem). L'amendement CL98, qui renvoie à la notion de « pratiques et standards internationaux communément admis », paraît préférable, et il a le mérite de distinguer clairement ce qui relève de la loi et du règlement.

*L'amendement CL33 est **retiré**.*

*L'amendement CL98 est **adopté**.*

*La commission émet un avis **favorable** à l'adoption de l'article 34 **modifié**.*

Article 35 (Art. L. 2321-2-1, L. 2321-3 et L. 2321-5 du code de la défense, art. L. 33-14, L. 36-7 et L. 36-14 du code des postes et des communications électroniques) *: Renforcement des capacités de détection des cyberattaques et d'information des victimes.*

Amendements de suppression CL12 de Mme Mélanie Thomin, CL14 de M. Philippe Latombe, CL37 de M. Ugo Bernalicis et CL69 de M. Aurélien Lopez-Liguori.

M. Roger Vicot (SOC). Nous ne sommes pas favorables à l'élargissement des missions de l'Anssi proposé par cet article. L'agence serait désormais chargée de détecter des attaques en recueillant des données auprès des opérateurs de télécommunication. Cette disposition paraît insuffisamment justifiée et encadrée. Cet élargissement des missions de l'Anssi pourrait, en outre, poser un problème de concurrence, en matière de contrôle, entre les services de renseignement, qui relèvent de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et l'Anssi qui, elle, relève de l'Arcep.

M. Philippe Latombe (Dem). Je fais confiance à la rapporteure pour avis et au ministre délégué chargé de la transition numérique et des télécommunications pour corriger les points problématiques dans les articles précédents.

En revanche, l'article 35 pose un problème d'équilibre et est en contradiction avec l'article L. 34-1 du code des postes et des télécommunications. Il concerne, en outre, un volume de données très important. Par ailleurs, même si on nous explique que le cache DNS

n'est pas une donnée personnelle identifiante, il permet quand même, quand on agrège les données, d'avoir une vision assez exhaustive de ce que quelqu'un a pu faire, soit sur un site, soit sur un serveur. On est assez proche de la définition que la Cour de justice de l'Union européenne avait donnée des métadonnées de connexion des opérateurs de téléphonie. Il est impératif de mieux encadrer l'article 35, si nous voulons qu'il soit constitutionnel et conventionnel.

M. Ugo Bernalicis (LFI-NUPES). Madame la rapporteure pour avis, lorsque nous avons examiné l'article 32, vous avez répondu à mon collègue Jérémie Iordanoff que nous faisions une confusion entre l'Anssi et les services de renseignement. Mais cet article confie, de fait, à l'Anssi, des missions qui relèvent du renseignement.

Au fond, je comprends votre logique : la menace est réelle et on a besoin de pouvoir l'anticiper en collectant des informations, pour ne pas être uniquement dans la réaction. Je ne suis pas sûr, cependant, que l'Anssi soit suffisamment dotée, en moyens, humains notamment, pour remplir cette mission. En outre, nous allons encore dépendre de solutions logicielles non souveraines.

Ces questions doivent être maniées avec force pincettes et, en l'état, l'article n'apporte pas les garanties suffisantes pour aller au-delà de la réglementation actuelle, laquelle permet déjà de faire des choses. Du reste, j'ose espérer que si les services de renseignement avaient connaissance d'une faille ou d'une menace quelconque, ils préviendraient aussitôt l'Anssi, pour que celle-ci fasse des contrôles plus poussés et écarte la menace.

M. Jordan Guitton (RN). Nous souhaitons, nous aussi, la suppression de cet article fourre-tout.

Si nous reconnaissons évidemment la nécessité de sauvegarder l'ordre public, les moyens proposés ici sont soit trop larges, soit flous, soit inutiles, soit inapplicables. Voulons-nous vraiment que des données de contenu soient transmises à l'Anssi sans décision d'un magistrat ni consultation de la Cnil ? La suppression de l'assermentation des agents habilités est-elle vraiment nécessaire ? L'Arcep a-t-elle la capacité opérationnelle d'assurer les missions qui lui seront confiées ? À toutes ces questions, la réponse est non. Dans son avis sur le présent projet de loi, l'Arcep a elle-même reconnu que « son organisation et son mode de fonctionnement ne lui permettent pas d'assurer une réactivité opérationnelle courte ».

Enfin, les mesures contenues dans l'article sont gravement attentatoires aux libertés et les garanties qui sont données ne nous convainquent pas. Nous en attendons une réécriture complète, plus respectueuse des libertés et plus précise. En attendant le débat en séance, nous demandons sa suppression.

Le Rassemblement national a toujours défendu la sécurité des biens et des personnes, par le renforcement des moyens des forces de sécurité, y compris grâce à de nouvelles technologies. Mais nous sommes aussi pour la sécurité des données, qui est essentielle à la sécurité de tous les Français. Or ce texte ne la garantit pas.

Mme Sabine Thillaye, rapporteure pour avis. Je rappelle que l'objectif de cet article n'est absolument pas la captation de données à caractère personnel, mais qu'il vise uniquement à mieux détecter une possible attaque, en récupérant les configurations et le détail des codes malveillants utilisés par l'attaquant, les données qu'il a dérobées, ses journaux de

connexion, ainsi que les éléments permettant de déchiffrer le trafic malveillant – toutes choses impossibles à détecter avec de simples marqueurs techniques.

Toutefois, j'entends vos inquiétudes et je veux vous dire que des garanties sont déjà prévues. Il y aura, d'abord, un ciblage préalable de la machine compromise faisant l'objet de la copie. Concrètement, l'Anssi devra motiver sa demande, en fournissant un dossier circonstancié analysant au préalable la menace qui justifie le recours à la technique de recueil. Je pense aussi au 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 considère que c'est justifié, 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.

J'ai sollicité l'Anssi, afin de connaître les volumes estimés de recours à l'article. S'agissant de dispositions enclenchées uniquement pour les menaces graves sur les administrations publiques et opérateurs stratégiques, l'Anssi estime que, sur une année, elle pourrait procéder à une cinquantaine de copies de serveurs et à une vingtaine de captations de flux réseaux, ce qui paraît proportionné à l'objectif de lutte contre les menaces à la sécurité nationale.

Dans la continuité du dispositif existant, plusieurs garanties sont maintenues. Les demandes ne portent que sur le périmètre d'opérateurs présentant une sensibilité particulière – autorités publiques, opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE) – et pour une durée limitée, et elles ont toujours 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 – nous reviendrons sur cette question. Enfin, la destruction immédiate des données par l'Anssi est prévue par notre droit, dès lors que celles-ci sont jugées inutiles pour la prévention et la caractérisation de la menace.

Je suis convaincue de l'utilité de cet article et ne suis donc pas favorable à sa suppression. Toutefois, pour répondre à vos inquiétudes, j'ai souhaité apporter quelques modifications et garanties complémentaires : d'abord, en exigeant des précisions sur le type de données faisant l'objet d'un recueil ; ensuite, en prévoyant la consultation de la Cnil avant la prise du décret ; enfin, en circonscrivant l'utilisation de l'article aux situations les plus graves menaçant la sécurité nationale.

M. Ugo Bernalicis (LFI-NUPES). Les alinéas 21 et 22 prévoient que l'Anssi pourra fournir des marqueurs techniques aux opérateurs et que c'est à eux qu'il reviendra de les exploiter et de signaler à l'agence des failles éventuelles. Vous introduisez donc une forme de sous-traitance. Cela me semble être un élément supplémentaire de porosité entre les opérateurs, qui ont leurs intérêts propres, et l'Anssi, qui travaille pour l'intérêt général et la protection de nos concitoyens et concitoyennes, de nos entreprises et de nos intérêts nationaux. Il me semble que les implications de cette disposition mériteraient un examen approfondi.

*La commission **rejette** les amendements.*

Amendement CL70 de M. Aurélien Lopez-Liguori (RN).

M. Jordan Guitton (RN). Nous proposons de supprimer les alinéas 2 à 9, qui donnent la possibilité à l'Anssi de recueillir des données de contenu. En cas de menace susceptible de porter atteinte à notre sécurité nationale, l'Anssi, qui dépend du SGDSN, placé

lui-même sous l'autorité de la Première ministre, pourrait recueillir une multitude de données sensibles qui transitent sur tous les réseaux. Le peu de garanties que vous proposez n'est pas de nature à nous rassurer, loin de là. L'Arcep, je l'ai dit, estime qu'elle n'aura pas les moyens d'assumer la nouvelle mission qui lui incombe. Enfin, les mesures proposées, intrusives, ne font pas l'objet d'une décision judiciaire préalable et ne sont pas assez encadrées. Le droit à la vie privée, au secret des communications et à la liberté d'expression sera toujours au cœur de nos préoccupations et nous ne cesserons jamais de les défendre, en accord avec la sécurité de nos compatriotes.

Suivant la préconisation de la rapporteure pour avis, la commission ***rejette*** *l'amendement.*

Amendements identiques CL34 de Mme Anne Le Hénanff et CL45 de M. Philippe Latombe.

Mme Anne Le Hénanff (HOR). Depuis la loi du 13 juillet 2018 relative à la programmation miliaire pour les années 2019 à 2025, en particulier en son article 34, les dispositions du code de la défense confèrent à l'Anssi le pouvoir de mettre en place, « lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques », des marqueurs techniques.

Eu égard au renforcement des capacités de détection de l'Anssi, laquelle devra soumettre à l'Arcep tout projet de collecte de données malveillantes, le présent amendement vise à s'assurer que la collecte de données ne s'effectuera qu'aux fins de garantir la défense et la sécurité nationale.

M. Philippe Latombe (Dem). Il faut absolument limiter la portée de l'article 35, en reprenant ce qui avait été fait dans l'article 34 de la précédente loi de programmation. Si nous ne le faisons pas, l'Anssi pourra poser des sondes sur des réseaux pour n'importe quel motif, sans limitation. Cette pratique est tellement attentatoire aux libertés qu'il faut absolument préciser sa finalité, à savoir garantir la défense et la sécurité nationales, et rien d'autre.

Mme Sabine Thillaye, rapporteure pour avis. Je partage votre objectif mais vous propose plutôt d'adopter l'amendement CL101, dont nous avons discuté hier avec le Gouvernement et le SGDSN et qui, me semble-t-il, a le même objectif que le vôtre. Je vous invite donc à retirer vos amendements.

M. Philippe Latombe (Dem). L'amendement CL101 n'a rien à voir avec les nôtres, puisqu'il évoque les « systèmes d'information » et ne concerne que la sécurité nationale. Or la défense et d'autres sujets sont aussi en cause.

Mme Sabine Thillaye, rapporteure pour avis. C'est une question que je me suis aussi posée. Je suis prête à retirer mon amendement au profit des vôtres.

La commission ***adopte*** *les amendements.*

L'amendement CL2 de Mme Mélanie Thomin est ***retiré****, de même que l'amendement CL101 de Mme Sabine Thillaye, rapporteure pour avis.*

Amendement CL3 de Mme Mélanie Thomin.

M. Roger Vicot (SOC). L'amendement vise à conditionner la mise en œuvre des marqueurs techniques à un avis conforme et préalable de l'Arcep. En effet, ces dispositifs de collecte particulièrement intrusifs appellent des garanties en matière de droits et de libertés publiques.

Mme Sabine Thillaye, rapporteure pour avis. Le dispositif juridique relatif aux marqueurs techniques prévoit déjà un contrôle *a posteriori* de l'Arcep. Il s'agit d'une possibilité qui existe depuis la précédente LPM, qui a été validée par le Conseil d'État, éprouvée par les acteurs, et que personne n'a remise en cause au cours des auditions que j'ai menées. J'estime utile de prévoir un avis *a priori* de l'Arcep dans le cadre du recueil de données, mais, s'agissant des marqueurs techniques, ce serait une restriction trop importante et injustifiée au regard des objectifs poursuivis, à savoir la protection de nos institutions et des opérateurs vitaux contre les cyberattaquants. Avis défavorable.

M. Roger Vicot (SOC). L'objectif poursuivi est louable mais il peut parfaitement s'articuler avec un avis préalable garantissant le respect des droits et libertés.

*La commission **rejette** l'amendement.*

*La commission **adopte** l'amendement rédactionnel CL82 de Mme Sabine Thillaye, rapporteure pour avis.*

Amendement CL4 de Mme Mélanie Thomin.

M. Roger Vicot (SOC). L'amendement vise à prévoir explicitement que les décisions prises en application de l'article 35 peuvent être soumises au juge administratif suivant la procédure du référé liberté, si les conditions tenant à l'urgence et à l'atteinte à une liberté fondamentale sont remplies.

Mme Sabine Thillaye, rapporteure pour avis. Avis défavorable, pour les mêmes raisons que celles avancées au sujet de votre amendement CL5, à l'article 32, qui concernait le même dispositif.

*La commission **rejette** l'amendement.*

Amendement CL94 de Mme Sabine Thillaye.

Mme Sabine Thillaye, rapporteure pour avis. Il conviendrait que le décret en Conseil d'État prévu à l'alinéa 9 soit pris après avis de la Cnil et de l'Arcep.

*La commission **adopte** l'amendement.*

Amendement CL97 de Mme Sabine Thillaye.

Mme Sabine Thillaye, rapporteure pour avis. Dans un souci de proportionnalité du dispositif, il est souhaitable que le décret d'application précise les informations et les catégories de données conservées.

*La commission **adopte** l'amendement.*

Amendements identiques CL13 de Mme Mélanie Thomin, CL35 de Mme Anne Le Hénanff, CL46 de M. Philippe Latombe, CL53 de Mme Clara Chassaniol, CL55 de Mme Gisèle Lelouis et CL93 de Mme Sabine Thillaye.

M. Roger Vicot (SOC). Il s'agit de maintenir l'exigence d'assermentation des agents de l'Anssi recueillant les données auprès des acteurs numériques. Puisque l'article étend le périmètre des données potentiellement recueillies, une garantie supplémentaire est nécessaire.

Mme Anne Le Hénanff (HOR). Si l'assermentation est exigée par le Conseil constitutionnel dans le seul cas où les agents concernés ont pour mission la recherche ou la poursuite d'infractions pénales, il serait préférable de la maintenir pour ceux de l'Anssi, eu égard au caractère particulièrement sensible des données concernées.

M. Philippe Latombe (Dem). Dans son avis, l'Arcep indique ne pas comprendre pourquoi le texte supprime l'assermentation. Nous devons écouter l'autorité de contrôle, d'autant plus que nous cherchons à instituer un dispositif proportionné, dont les finalités sont précisément circonscrites. Il faut absolument maintenir ce lien de confiance avec l'agence, qui est un service administratif et non une autorité indépendante.

Mme Clara Chassaniol (RE). Nos débats attestent le caractère sensible des données auxquelles ont accès les agents de l'Anssi. Il est nécessaire de conserver l'assermentation pour maintenir la confiance dans l'agence.

Mme Gisèle Lelouis (RN). Je me réjouis que l'article 35 confère enfin partiellement à l'Anssi la capacité de disposer de capteurs informatiques au sein d'infrastructures variées pour détecter et contrer les cyberattaques, ainsi que de communiquer des données à d'autres services de l'État, notamment aux services de renseignement. Toutefois, soucieuse de la sécurité des systèmes d'information des autorités publiques et des opérateurs, je souhaite, par cet amendement, maintenir l'assermentation des agents prévue par le code de la défense.

Vous entendez la supprimer, alors que ces personnes ont un niveau d'habilitation particulier. Par cette disposition, je discerne la volonté de supprimer des postes. Je m'inquiète pour ces agents qui risquent de perdre leur travail et me demande qui les remplacera avec autant d'efficacité. N'y a-t-il pas là une volonté de contourner les spécialistes pour agir selon votre bon vouloir ? Des abus ou erreurs sont à craindre, puisque ce ne seront plus des agents ayant prêté serment pour accomplir une tâche particulière qui se consacreront à celle-ci mais des personnes habilitées, peut-être moins formées et moins protégées.

Par cet amendement, je souhaite protéger les agents comme les Français.

Mme Sabine Thillaye, rapporteure pour avis. L'assermentation des agents est une garantie exigée pour ceux d'entre eux qui sont chargés de rechercher ou de poursuivre des infractions pénales, ce qui n'est pas le cas des agents de l'Anssi visés par l'article. Selon l'étude d'impact, l'assermentation, qui constitue une procédure lourde, s'applique à la quasi-totalité des personnels de la sous-direction des opérations de l'Anssi, soit près de 200 agents sur un total de 280. Cela étant dit, j'entends les craintes que cet article peut inspirer, bien qu'il soit assorti de garanties. Aussi suis-je favorable, comme vous, au maintien de l'assermentation des agents de l'Anssi.

*La commission **adopte** les amendements.*

*Elle **adopte** successivement les amendements rédactionnels CL83, CL84, CL86 et CL85 de Mme Sabine Thillaye, rapporteure pour avis.*

*La commission émet un avis **favorable** à l'adoption de l'article 35 **modifié**.*

Après l'article 35

Amendements identiques CL17 de Mme Anne Le Hénanff et CL38 de M. Philippe Latombe.

Mme Anne Le Hénanff (HOR). Il s'agit de rendre obligatoires, pour les opérateurs d'importance vitale et de services essentiels, l'identification de leurs données sensibles et la prise de mesures techniques ou opérationnelles pour protéger ces dernières. La protection des données sensibles, qui plus est de ces opérateurs, est un enjeu majeur qui s'inscrit dans la démarche de souveraineté numérique du Gouvernement.

Cet amendement traduit une attente réelle de la part de l'ensemble des acteurs de l'écosystème, mais aussi de parlementaires qui travaillent sur le sujet depuis plusieurs années. À titre personnel, je souhaite que nous inscrivions rapidement dans la loi une telle disposition. Je me tiens à la disposition de la rapporteure pour avis pour travailler, en vue de la séance, à une réécriture de cet amendement, que je retire.

M. Philippe Latombe (Dem). J'évoquerai trois cas. Doctolib est hébergé par une plateforme américaine. Si, dans le cadre des règlements DSA (Digital Services Act) et DMA (Digital Markets Act), dont nous allons être saisis par le ministre délégué chargé de la transition numérique dans quelques jours, Amazon Web Services bloquait l'accès aux données de Doctolib à la suite d'un conflit commercial avec cette société, comment ferions-nous pour prendre des rendez-vous, en médecine de ville comme à l'hôpital ? Les propositions qui sont faites pour garantir notre souveraineté nous prémuniraient contre le risque de blocage d'un opérateur de services essentiels tel que Doctolib. Deuxième exemple : Palantir, logiciel qui a été financé à l'origine par la CIA, est aujourd'hui utilisé par des opérateurs français, notamment Airbus. Si un conflit commercial survenait avec Boeing, la dépendance à un opérateur de ce type, qui dispose d'informations stratégiques sur Airbus, soulèverait la question de notre souveraineté économique. Troisième exemple, le *Health Data Hub*, qui est hébergé par Microsoft. Le Gouvernement avait promis, il y a deux ans, un basculement vers un cloud souverain, mais l'administration n'a pas tenu la promesse. Il semble donc nécessaire de l'inscrire dans la loi pour imposer la réversibilité. Il nous faudra, en séance publique, prévoir l'élaboration d'un plan de réversibilité, par décret, en 2023 et fixer le délai d'application à la fin 2024.

Mme Sabine Thillaye, rapporteure pour avis. Je partage, comme beaucoup de nos collègues, l'objectif de votre amendement. C'est d'ailleurs grâce à vous qu'une discussion s'est semble-t-il engagée à Bercy afin de répondre à la préoccupation que vous soulevez. Toutefois, il s'agit d'un dispositif très lourd, qui n'a pas été expertisé et dont je n'ai pas pu me faire une idée précise. Ce qui est certain, c'est qu'il entraînerait des coûts importants et aurait des conséquences en termes de concurrence qui doivent être mesurées. Je donnerai un avis défavorable tout en vous invitant à retravailler le dispositif en vue de la séance.

M. Aurélien Lopez-Liguori (RN). Cet amendement vise à identifier les données stratégiques qui ne doivent pas être captées par des pays étrangers et à faire en sorte que leur traitement soit opéré par une entreprise française ou européenne. Il est le bienvenu dans une loi de programmation militaire qui évoque très peu la souveraineté dans le domaine cyber, bien que le sujet soit crucial. Comme nous l'affirmons depuis des années au Rassemblement national, souveraineté et sécurité sont les deux faces d'une même pièce. Nous ne pouvons accepter que des administrations, institutions et autorités publiques françaises constituant des opérateurs d'importance vitale hébergent leurs données auprès d'entreprises américaines, chinoises ou relevant d'autres pays extra-européens. Ces sociétés peuvent être soumises à l'extraterritorialité du droit de leur pays, ce qui signifie qu'en bout de chaîne, des gouvernements étrangers pourraient mettre la main sur des données sensibles de l'État français. Cet amendement est très important ; il pourrait changer la donne pour nos entreprises. Nous le voterons.

M. Raphaël Schellenberger (LR). Je salue le travail mené depuis plusieurs années par Philippe Latombe, comme par d'autres collègues, sur la souveraineté numérique. C'est un enjeu stratégique pour notre économie et plus encore pour les données sensibles et la protection de chacun de nos concitoyens. L'exemple médical est le meilleur qui soit. La réalisation de l'étude d'impact ne demanderait pas beaucoup de temps : il suffit de regarder ce que nos voisins européens ont fait. Il n'y a pas de raison que nous ne puissions pas les imiter. Nous disposons d'un véhicule législatif et avons deux semaines, d'ici à la séance, pour retravailler le dispositif. Il est important que nous actions, dès la commission, que le sujet doit figurer dans le texte. Vous trouverez Les Républicains à vos côtés, en séance pour effectuer les corrections à la marge qui s'imposent.

L'amendement CL17 est ***retiré****.*

La commission ***adopte*** *l'amendement CL38.*

La commission émet un avis ***favorable*** *à l'adoption de l'ensemble des dispositions dont elle est saisie,* ***modifiées****.*

La séance est levée à 15 heures 30.

Membres présents ou excusés

Présents. - Mme Sabrina Agresti-Roubache, M. Ugo Bernalicis, Mme Clara Chassaniol, M. Guillaume Gouffier Valente, M. Jordan Guitton, M. Sacha Houlié, M. Timothée Houssin, M. Jérémie Iordanoff, M. Philippe Latombe, M. Antoine Léaument, Mme Gisèle Lelouis, Mme Marie-France Lorho, M. Emmanuel Mandon, Mme Élisa Martin, M. Thomas Ménagé, M. Ludovic Mendes, M. Stéphane Rambaud, Mme Sandra Regol, M. Thomas Rudigoz, M. Raphaël Schellenberger, Mme Sarah Tanzilli, Mme Sabine Thillaye, M. Roger Vicot

Excusés. - M. Romain Baubry, Mme Blandine Brocard, M. Éric Ciotti, Mme Marie Guévenoux, M. Mansour Kamardine, Mme Marietta Karamanli, Mme Emeline K/Bidi, Mme Julie Lechanteux, Mme Naïma Moutchou, Mme Danièle Obono, M. Thomas Portes, M. Davy Rimane

Assistait également à la réunion. - Mme Anne Le Hénanff