ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Mardi 9 septembre 2025
Séance de 21 heures 30

Compte rendu n° 18

SESSION EXTRAORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à vingt et-une heures trente.

La commission spéciale a poursuivi l'examen du projet de loi, adopté par le Sénat après engagement de la procédure accélérée, relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (n° 1112) (M. Éric Bothorel, rapporteur général, Mme Catherine Hervieu, Mme Anne Le Hénanff, M. Mickaël Bouloux, rapporteurs).

M. le président Philippe Latombe. Mes chers collègues, nous poursuivons l'examen du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Article 13 : *Absence d'application des dispositions du projet de loi aux entités soumises à des exigences équivalentes en application d'un acte juridique de l'Union européenne*

Amendements identiques CS493 de M. Éric Bothorel et CS316 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure pour le titre II. Il s'agit de clarifier les dispositions qui ne trouvent pas à s'appliquer dans le cas d'un acte sectoriel de l'Union européenne reconnu comme *lex specialis* qui prévoit des dispositions équivalentes. Il tend ainsi à préciser que sont uniquement concernées les dispositions relatives à l'application de mesures de sécurité, à la notification des incidents ainsi qu'à celle de la supervision permettant d'en vérifier le respect. En dehors de ces dispositions, les entités restent soumises au projet de loi, s'agissant par exemple de l'obligation d'enregistrement issue de l'article 12, dont elles ne sont pas déliées.

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

Amendement CS317 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à compléter l'article 13 par l'alinéa suivant : « Tous les deux ans, l'Agence nationale de sécurité des systèmes d'information publie et actualise des lignes directrices d'analyse des différentes réglementations européennes permettant de hiérarchiser le degré d'exigence de chacune pour les entités concernées. »

De nombreuses réglementations numériques, sectorielles et non sectorielles, s'imposent aux entreprises. Disposer d'un référentiel piloté par l'Agence nationale de la sécurité des systèmes d'information (Anssi) permet de s'assurer du respect de la hiérarchie des exigences. Il ne s'agit pas d'alourdir la charge de l'Anssi en communiquant à chaque entreprise la hiérarchisation des normes qui s'impose à elle, mais de fixer des lignes directrices auxquelles chacun pourra se référer pour en faciliter le respect.

Mme Anne Le Hénanff, rapporteure. Publier des lignes directrices n'est pas le rôle de l'Anssi. Par ailleurs, les entités concernées disposent souvent de services juridiques capables d'assurer une veille. Peut-être est-ce davantage le rôle de la Commission européenne ou de l'Agence européenne de cybersécurité (Enisa). Avis défavorable.

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

*Elle **adopte** l'article 13 **modifié**.*

Article 14 : *Mise en place de mesures de cybersécurité par les entités essentielles et importantes*

Amendements identiques CS528 de M. Éric Bothorel et CS322 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il s'agit d'exclure explicitement du champ d'application de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite directive NIS 2, les activités liées à la sécurité nucléaire, pour lesquelles la France souhaite pouvoir exercer pleinement et entièrement sa compétence exclusive en matière de sauvegarde de la sécurité et de la souveraineté nationales, tout en conservant leur assujettissement à un niveau d'exigence rigoureusement équivalent à celui prévu par la directive.

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

Amendement CS453 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il prévoit que les entités listées à l'alinéa 1 de l'article 14 mettent en œuvre à leurs frais les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services.

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement.*

*En conséquence, les amendements CS339 et CS340 de Mme Anne Le Hénanff, rapporteure **tombent**.*

Amendement CS186 de Mme Marie Récalde

Mme Marie Récalde (SOC). Compte tenu du débat sur l'approche « tous risques » que nous avons eu lors de l'examen de l'article 6, nous le retirons.

*L'amendement est **retiré**.*

*Suivant l'avis du rapporteur général, la commission **adopte** successivement les amendements rédactionnels CS320 et CS321 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS319 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à ajouter, à la deuxième phrase de l'alinéa 1, les mots « et de résilience » après le mot « sécurité » afin de préciser que les mesures techniques et organisationnelles précitées garantissent, pour les réseaux et les systèmes d'information des entités concernées, un niveau de résilience adapté et proportionné au risque.

Mme Anne Le Hénanff, rapporteure. L'introduction de la notion de résilience me semble opportune compte tenu de son caractère indispensable. Avis favorable.

M. Éric Bothorel, rapporteur général. Sagesse.

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

Amendement CS318 de M. Philippe Latombe

M. le président Philippe Latombe. L'amendement vise à modifier de façon assez substantielle l'article 14 en introduisant, après la deuxième phrase de l'alinéa 1, la phrase suivante : « Le choix de ces mesures tient compte de leur capacité à être auditées, de la transparence de leur fonctionnement, de leur interopérabilité, de leur résilience et de la maîtrise qu'elles permettent d'acquérir sur les systèmes d'information afin de minimiser les dépendances technologiques à l'égard de prestataires tiers ne présentant pas de garanties suffisantes de conformité aux exigences de cybersécurité et de souveraineté numérique telles que fixés par la stratégie nationale dans une perspective de long terme ».

Mme Anne Le Hénanff, rapporteure. Ces critères sont intéressants mais très lourds à mettre en œuvre. Par ailleurs, l'amendement surtranspose la directive NIS 2. Avis défavorable.

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

*Puis elle **adopte** les amendements rédactionnels CS326 et CS327 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS324 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise, par cohérence avec l'alinéa 5, à compléter l'alinéa 2 par les mots « en fonction de leur degré d'exposition au risque ». Le projet de loi prévoit, dans sa version initiale, que les entités doivent mettre en œuvre un pilotage adapté de la sécurité des réseaux et des systèmes d'information, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques.

Le Sénat, considérant que ce texte transpose insuffisamment l'article 20 de la directive NIS 2, a renforcé à juste titre ces dispositions afin que les mesures prévues garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté et proportionné aux risques. Toutefois, la rédaction adoptée par le Sénat n'est pas homogène avec le reste de l'article, notamment avec l'alinéa 5, ce qui risque de créer une ambiguïté.

Mme Anne Le Hénanff, rapporteure. Sagesse.

M. Éric Bothorel, rapporteur général. Sagesse également.

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

Amendement CS325 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à rappeler l'objectif de souveraineté numérique dans le processus de certification.

Mme Anne Le Hénanff, rapporteure. Mentionner la « souveraineté numérique » est une mesure de cohérence à l'article 5 *bis* mais de surtransposition ailleurs.

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

Amendement CS323 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à compléter l'alinéa 2 par la phrase suivante : « Le choix d'une solution logicielle dont le code source n'est pas accessible ou vérifiable, et lorsqu'elle concerne un système d'information critique, fait l'objet d'une analyse de risques spécifique, documentée et présentée aux organes de direction évaluant la dépendance vis-à-vis du fournisseur, les limitations en matière d'audit de sécurité et les stratégies de réversibilité à brève échéance ». Il s'agit de s'assurer qu'il n'y a pas de dépendance technologique rendant prisonnier d'un fournisseur unique et de se prémunir de toute opacité dans la mesure où l'impossibilité de faire réaliser un audit complet du code source constitue un risque de sécurité intrinsèque.

S'agissant de la souveraineté des données et des systèmes, le présent amendement s'inscrit dans la continuité de l'article 16 de la loi pour une République numérique, qui dispose : « Les administrations mentionnées au premier alinéa de l'article L. 300-2 du code des relations entre le public et l'administration veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information ». L'amendement permet de préciser cette exigence s'agissant des infrastructures critiques du pays.

Mme Anne Le Hénanff, rapporteure. L'amendement surtranspose la directive NIS 2. Avis défavorable.

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

Amendement CS328 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement de clarification vise à ajouter, à l'alinéa 3, les mots « et la résilience » après le mot « protection ».

Mme Anne Le Hénanff, rapporteure. S'agissant d'une disposition relative à la résilience, j'émets un avis favorable.

M. Éric Bothorel, rapporteur général. La résilience figure expressément à l'alinéa 1 du présent article, au rang des objectifs que doivent viser les mesures qu'il prévoit. Avis défavorable.

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

Amendement CS329 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à compléter l'alinéa 4 par les mots « et la transparence ainsi que la capacité des technologies utilisées à être auditées afin de faciliter l'investigation et la résolution desdits incidents ». Il s'agit d'une part d'introduire dans l'article les notions d'auditabilité, de transparence, de portabilité et d'interopérabilité des technologies choisies par les entités essentielles et les entités importantes afin de réduire le risque de dépendance numérique, de maximiser la résilience des réseaux et des systèmes, de permettre la continuité des activités et, d'autre part, de rappeler l'objectif de souveraineté numérique dans le processus de certification.

Mme Anne Le Hénanff, rapporteure. L'amendement aurait pour effet de surtransposer la directive ; avis défavorable.

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

*Suivant l'avis de la rapporteure, elle **rejette** l'amendement CS220 de M. Aurélien Lopez-Liguori.*

Amendement CS454 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il vise à compléter l'alinéa 5 afin de préciser que les entités listées à l'alinéa 1 prennent les mesures nécessaires pour garantir la résilience des réseaux et des systèmes d'information.

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

Amendement CS330 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à compléter l'alinéa 5 par les mots « en favorisant la libre intégration et l'interopérabilité des technologies et protocoles utilisés, ainsi que la portabilité des données » pour introduire dans l'article les notions d'auditabilité, de transparence, de portabilité et d'interopérabilité des technologies choisies par les entités essentielles et importantes.

Mme Anne Le Hénanff, rapporteure. Surtransposition de la directive ; avis défavorable.

M. Éric Bothorel, rapporteur général. Même avis, malgré l'importance du sujet.

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

Amendement CS219 de M. Aurélien Lopez-Liguori

Mme Anne Le Hénanff, rapporteure. Je comprends l'intérêt de cet amendement mais il aurait pour effet de surtransposer la directive. Avis défavorable.

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

Amendement CS331 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à substituer aux alinéas 6 à 8 neuf alinéas réécrivant certaines dispositions. Dans le texte d'origine, seules l'élaboration, la modification et la publication d'un référentiel d'exigences techniques et organisationnelles sont soumises à la concertation des parties prenantes, qui par ailleurs n'incluent pas les ministères coordinateurs. Il s'agit de les inclure dans le référentiel, de même que les guides de l'Enisa.

Mme Anne Le Hénanff, rapporteure. Je suggère le retrait de l'amendement au profit de l'amendement suivant ; à défaut, avis défavorable.

L'amendement est ***retiré****.*

Amendement CS456 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il s'agit d'ajouter les ministères à la liste des personnes avec lesquelles l'Anssi se concertera pour l'élaboration, la modification et la publication du référentiel d'exigences techniques et organisationnelles d'une part et, d'autre part, de procéder à des modifications d'ordre rédactionnel.

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

Amendement CS333 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement d'appel vise à préciser à l'alinéa 7 que le recours aux produits, services et processus certifiés est prescrit prioritairement par le référentiel et subsidiairement par l'Anssi, afin de parvenir à un équilibre entre la norme européenne de l'Enisa, garante d'homogénéité avec les pays voisins de la France, et le savoir-faire reconnu de l'Anssi.

Mme Anne Le Hénanff, rapporteure. Je suggère le retrait de l'amendement au profit de l'amendement CS337 ; à défaut, avis défavorable.

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

Amendement CS334 de M. Philippe Latombe

M. le président Philippe Latombe. Il s'agit de modifier l'alinéa 7 pour faire dépendre le recours à des produits, à des services ou à des processus certifiés de la réalisation d'une étude de risque de dépendance stratégique afférent.

Mme Anne Le Hénanff, rapporteure. Surtransposition ; avis défavorable.

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

Amendement CS221 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). L'article 14 permet de recourir à des solutions certifiées au titre du règlement CSA – le Cyber Security Act. Or une faille demeure. L'immunité face aux droits extraterritoriaux étrangers n'est pas garantie. Si nous acceptons que des prestataires soumis à des législations étrangères puissent obtenir une certification européenne, alors nous aurons une sécurité d'étiquette mais pas une sécurité réelle. Le présent amendement propose une clarification simple : les services certifiés que l'État pourra prescrire doivent être établis en Europe. Notre autonomie stratégique doit dépendre de nos lois uniquement.

Mme Anne Le Hénanff, rapporteure. Surtransposition ; avis défavorable.

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

Amendement CS336 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à préciser que les produits, services et processus certifiés peuvent faire l'objet d'un audit et répondent à des critères de transparence et que priorité est donnée aux solutions présentant le plus haut niveau de transparence, d'ouverture et de la réversibilité.

Mme Anne Le Hénanff, rapporteure. Surtransposition ; avis défavorable.

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

Amendements CS337 de Mme Anne Le Hénanff et CS152 de Mme Marina Ferrari (discussion commune)

Mme Anne Le Hénanff, rapporteure. L'amendement CS337 vise à remplacer, à l'alinéa 8, une formulation générique par une référence explicite à la directive NIS 2. Cette clarification garantit une articulation cohérente entre le cadre européen et le dispositif national élaboré par l'Anssi, prévu par décret en Conseil d'État, à l'attention des entités visées à l'alinéa 1. Une telle mention prévient toute ambiguïté, évite les interprétations divergentes et limite les risques de surtransposition.

Mme Marina Ferrari (Dem). Je retire l'amendement CS152 au profit du CS337.

M. Éric Bothorel, rapporteur général. Sagesse.

*L'amendement CS152 est **retiré**.*

*La commission **adopte** l'amendement CS337.*

Amendements identiques CS529 de M. Éric Bothorel et CS338 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Le présent amendement a pour objectif d'offrir aux entités régulées la possibilité de se prévaloir du recours à certaines prestations de services qualifiés pour faciliter la démonstration de leur respect complet ou partiel des objectifs de sécurité. Il répond aux préoccupations émises par la commission spéciale relatives à l'encadrement du recours aux prestataires qualifiés. Il permet de valoriser le recours par les entités assujetties aux prestations qualifiées par l'Anssi et de favoriser le développement de l'offre de confiance sans l'imposer aux entités régulées.

L'approche incitative dont il procède constitue une manière équilibrée de répondre à ces préoccupations. Les entités régulées pourront, en fonction de leurs besoins, identifier les solutions qu'elles considèrent comme adéquates à leurs enjeux. Les conditions d'application des dispositions introduites par le présent amendement seront prévues par décret en Conseil d'État.

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

*Elle **adopte** l'article 14 **modifié**.*

Après l'article 14 :

Amendement CS59 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Il vise à rappeler la nécessité de recourir, dans la mesure du possible, aux logiciels libres et aux services de cloud réversibles afin de renforcer la sécurité des données collectées.

L'usage de logiciels libres présente de nombreux atouts. Leur coût est minime, voire nul. Ils peuvent facilement être modifiés et personnalisés pour répondre à des besoins spécifiques. Ils sont plus transparents et plus éthiques que les autres, et surtout plus sûrs, car ils sont souvent examinés par une communauté de développeurs spécialisés qui peuvent identifier et corriger les vulnérabilités signalées par les utilisateurs plus rapidement qu'avec les logiciels propriétaires.

Quant aux services de cloud réversibles, ils permettent de préserver une autonomie technologique et d'assurer la sécurité en donnant la faculté de récupérer les données stockées à tout moment pour assurer la protection des données personnelles collectées.

Les administrations publiques devraient utiliser ces outils libres et transparents pour assurer au mieux la protection des données personnelles qu'elles collectent dans le cadre de leurs activités, garantissant ainsi les droits fondamentaux des citoyens et la souveraineté technologique européenne.

Mme Anne Le Hénanff, rapporteure. Cet amendement ne transpose pas la directive NIS 2. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). Nous avons en France un écosystème très compétent qui n'est pas exclusivement basé sur des logiciels libres et qui a besoin de la commande publique. Cantonner la stratégie d'équipement de nos administrations aux logiciels libres n'est donc pas une bonne solution.

M. Arnaud Saint-Martin (LFI-NFP). Nous ne proposons pas une contrainte mais une simple orientation pour compléter l'offre et promouvoir l'usage des logiciels libres.

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

Amendement CS148 de M. Philippe Latombe

Mme Sabine Thillaye (Dem). Il vise à intégrer dans les règles encadrant le recours à des prestataires non européens la possibilité de travailler avec des entreprises établies dans les pays ayant un accord de commerce et de coopération avec l'Union européenne, à condition qu'elles acceptent explicitement d'être soumises aux normes européennes en matière de cybersécurité et de protection de données.

Il s'agit de trouver un équilibre entre la protection de la souveraineté numérique et l'ouverture à des partenaires fiables, tout en renforçant l'attractivité internationale de la mise en conformité avec les standards européens.

Mme Anne Le Hénanff, rapporteure. Ce sujet n'est pas traité dans la directive. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). L'argument de la surtransposition a ses limites. Cette directive prouve que l'Union européenne n'a rien à faire de la souveraineté numérique des États membres – on l'avait d'ailleurs déjà vu avec la loi Sren – puisqu'elle ne s'inquiète pas que la cybersécurité européenne soit assurée par des entreprises américaines, canadiennes ou autres.

En tant que législateur français, nous devons prendre des décisions pour notre pays. Je ne vois pas en quoi ces mesures de protection posent problème : elles ne vont pas à l'encontre de la directive, elles vont juste un peu plus loin et elles ne créent pas de problèmes de concurrence.

Mme Anne Le Hénanff, rapporteure. En l'occurrence, je n'ai pas parlé de surtransposition ; au contraire, ces mesures ne transposent pas la directive.

C'est certes un sujet important, mais il n'a pas sa place dans ce texte.

M. Éric Bothorel, rapporteur général. La directive NIS 2, qui vise à élever le niveau de cybersécurité de nos entités les plus critiques en imposant à l'ensemble de leurs systèmes d'information des exigences de sécurité proportionnées, ne prévoit pas de conditions supplémentaires quant au recours à des prestataires établis dans les pays tiers. Imposer à l'ensemble des entités régulées de telles conditions apparaît comme disproportionné et représenterait un coût majeur pour les entreprises françaises, qui seraient défavorisées par rapport à leurs concurrentes européennes.

Cette disposition serait par ailleurs contraire au droit européen.

Enfin, il n'existe aujourd'hui aucun mécanisme en matière de cybersécurité équivalent au mécanisme d'adéquation du règlement général sur la protection des données (RGPD).

Pour toutes ces raisons, je suis également défavorable à l'amendement.

Mme Sabine Thillaye (Dem). Je comprends vos arguments mais il arrive qu'en l'absence de prestataires compétents en France, nos entreprises n'aient pas d'autre choix que de recourir à des prestataires étrangers. L'amendement, en exigeant le respect des règles européennes, permettrait d'assurer un minimum de sécurité.

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

Amendements CS32 et CS33 de Mme Sabine Thillaye (discussion commune)

Mme Sabine Thillaye (Dem). Pour faire face à la multiplication des cyberattaques, qui ciblent aussi les collectivités locales, l'amendement CS32 introduit une obligation pour les communautés de communes de se doter d'un responsable de la sécurité des systèmes d'information (RSSI).

L'amendement de repli CS33 prévoit que les communautés de communes désignent au moins un référent cybersécurité, au besoin mutualisé.

Mme Anne Le Hénanff, rapporteure. Nous ne pouvons pas contraindre les intercommunalités à se doter d'un RSSI, notamment en raison de son coût salarial. La directive ne décrit pas aussi finement les obligations de moyens ; elle prévoit plutôt des obligations de résultats.

Il est préférable de laisser les territoires s'organiser. Il existe par exemple des associations de RSSI qui partagent leur temps entre plusieurs collectivités.

Avis défavorable.

M. Éric Bothorel, rapporteur général. J'ajoute que les salaires de ces professionnels sont élevés – parfois à six chiffres – et qu'il existe une concurrence forte pour les recruter. En outre, par les temps qui courent, il est sans doute préférable de s'abstenir de faire des entorses à la libre administration des collectivités.

Mme Sabine Thillaye (Dem). Je comprends vos arguments pour le RSSI, mais un référent dont la mission serait notamment de sensibiliser ne me semble pas inutile. Nous pourrions nous inspirer des correspondants défense.

Mme Anne Le Hénanff, rapporteure. L'analogie est intéressante. Nous pourrions imaginer que le référent cybersécurité dans une intercommunalité soit l'élu en charge du numérique, voire le maire, puisque c'est lui qui est responsable pénalement et qui pilote la gouvernance de la cybersécurité.

Mme Sabine Thillaye (Dem). Les communes ont l'obligation de se doter d'un correspondant défense. Il n'existe pas d'obligation similaire en matière de cybersécurité.

Mme Catherine Hervieu (EcoS). Il me semble plus judicieux que le référent soit un administrateur issu de la préfecture, car les élus ne sont ni élus *ad vitam aeternam* ni spécialistes de tous les sujets.

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

Amendements CS19 de Mme Sabine Thillaye

Mme Sabine Thillaye (Dem). Afin de renforcer la résilience des infrastructures et de faire face à la rapidité des évolutions technologiques, cet amendement propose d'imposer aux entités essentielles et aux entités importantes la réalisation par un organisme qualifié d'un audit complet de cybersécurité tous les quatre ans. Cette disposition s'inspire de l'Allemagne, où les audits peuvent être exigés tous les trois ans.

Mme Anne Le Hénanff, rapporteure. Les entités essentielles et les entités importantes concernées par NIS 2 seront tenues de faire un état des lieux de leur cybersécurité, soit par des audits *flash*, soit à l'initiative de l'Anssi ou de ses représentants dans les territoires. Votre amendement est donc satisfait.

M. Éric Bothorel, rapporteur général. La réalisation de tels audits représenterait une charge financière et opérationnelle supplémentaire qui ne me semble pas nécessaire. Par ailleurs, l'obligation d'auditer à intervalles planifiés et proportionnés est prévue au niveau réglementaire. Ensuite, le marché de l'audit en cybersécurité n'a pas, en l'état, la capacité d'absorber une telle demande.

Enfin, la procédure de contrôle prévue par cet amendement ferait doublon avec celle prévue aux articles 29 et 31 et ne présente pas les garanties procédurales associées. Ces articles prévoient déjà que l'Anssi a la capacité, lors d'un contrôle, de réaliser ou de faire réaliser par un organisme indépendant des audits réguliers et ciblés et d'enjoindre à l'entité, en cas de manquement, de prendre les mesures nécessaires. Avis également défavorable.

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

Article 15 *Opposabilité à l'ANSSI en cas de contrôle de ma mise en œuvre du référentiel d'exigences techniques et organisationnelles*

Amendements CS341, CS342, CS343 de M. Philippe Latombe (discussion commune)

M. le président Philippe Latombe. L'amendement CS341 propose d'inverser la charge de la preuve du respect des objectifs de sécurité et de ne pas la faire reposer sur l'assujetti, conformément à la position d'autres pays européens ayant transposé la directive.

L'inversion de la preuve permet également des gains financiers à la fois pour les entités régulées mais aussi pour l'État lors des opérations de contrôle qui sont de fait simplifiées.

Les amendements CS342 et CS343 sont des amendements de repli.

Mme Anne Le Hénanff, rapporteure. Je vous propose de retirer vos amendements au profit des amendements de réécriture que j'ai déposés avec le rapporteur général.

*Les amendements CS342 et CS343 sont **retirés**.*

*La commission **rejette** l'amendement CS341.*

Amendements CS344 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement propose que le référentiel technique de l'Enisa puisse être utilisé comme référence par les personnes visées à l'alinéa 1 de l'article 14 afin de permettre une meilleure coordination entre les réglementations européennes.

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

Amendements identiques CS530 de M. Éric Bothorel et CS457 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement procède à une réécriture quasi complète de l'article 15 afin de clarifier les conditions dans lesquelles seront reconnues les normes et spécifications techniques, européennes ou internationales permettant aux entités régulées de démontrer leur conformité, partielle ou totale, aux objectifs visés. Il tend par ailleurs à faciliter, pour les entités établies dans plusieurs pays de l'Union européenne, la reconnaissance de leur conformité, partielle ou totale, aux objectifs visés lorsqu'elles appliquent un autre référentiel que celui de l'Anssi.

M. Aurélien Lopez-Liguori (RN). La France sera l'un des États les mieux-disants pour l'application de la directive. C'est une très bonne chose. Mais, en présumant la conformité jusqu'à preuve du contraire, ne risque-t-on de mettre nos entreprises en concurrence avec des entreprises hongroises, hollandaises ou polonaises pénétrant notre marché alors que ces pays font une application plus laxiste de la directive ?

M. Éric Bothorel, rapporteur général. Je ne vois pas comment des acteurs moins-disants pourraient bénéficier d'un label de confiance. Nous sommes dans une logique de simplification et d'efficacité, qui est fortement demandée, et je crois que nous avons trouvé le point d'équilibre ; je ne redoute pas une quelconque menace hongroise ou autre sur notre écosystème.

*La commission **adopte** les amendements ; en conséquence, l'amendement CS346 de Mme Anne Le Hénanff **tombe**.*

Amendement CS345 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement vise à ouvrir la discussion sur la reconnaissance de l'équivalence des référentiels publiés par l'Enisa et par les organismes homologues de l'Anssi dans d'autres pays européens, par exemple en Allemagne, en Belgique ou encore en Espagne.

Mme Anne Le Hénanff, rapporteure. Avis défavorable.

M. Éric Bothorel, rapporteur général. La rédaction proposée, qui mentionne « tout organisme européen » ne semble pas suffisamment sécurisante. Il serait préférable de la limiter aux autorités compétentes d'autres États membres de l'Union européenne ou aux organismes ayant fait l'objet d'une accréditation par un organisme tel que le Comité français d'accréditation (Cofrac). Par ailleurs, les termes « référentiels et exigences équivalents » ne sont pas suffisamment clairs.

À titre d'exemple, avec votre rédaction, une société de conseil exerçant ses activités au sein de plusieurs États membres de l'Union européenne et qui recommanderait un référentiel reconnu pourrait approuver ces labels de confiance. Avis défavorable.

M. le président Philippe Latombe. Je retire l'amendement pour le retravailler avant la séance.

*L'amendement est **retiré**.*

*La commission **adopte** l'article 15 **modifié**.*

Article 16 *Exigences de protection cyber supplémentaires pour les OIV et pour les administrations*

*La commission **adopte** successivement les amendements rédactionnels CS347, CS348, CS349 et CS350 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS495 de M. Éric Bothorel et CS352 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement vise à corriger une erreur rédactionnelle suite à la reprise textuelle de l'article 14 du projet de loi. En tant qu'établissement public à caractère industriel et commercial, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) n'est en effet pas concerné par les exigences spécifiques fixées par le premier ministre à l'égard des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations.

Ces exigences ne concernent que les administrations qui sont des entités essentielles ou importantes, les administrations de l'État et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, de la répression pénale, ou des missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information, et enfin les juridictions administratives et judiciaires.

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

*Suivant l'avis de la rapporteure, elle **adopte** l'amendement rédactionnel CS351.*

Amendements identiques CS353 de M. Philippe Latombe et CS239 de M. Aurélien Lopez-Liguori

M. le président Philippe Latombe. L'amendement vise à prendre en compte le rôle stratégique des systèmes de détection des menaces en permettant, comme pour les opérateurs d'importance vitale (OIV), la définition d'exigences spécifiques pour ces services et solutions. Il s'agit de prévoir des obligations strictes en matière de notification des incidents pour rendre l'utilisation des systèmes de détection de menaces plus performants.

L'État définira des exigences spécifiques pour les systèmes de détection des menaces, qui pourront être mises en œuvre grâce à la qualification déjà existante de l'Anssi pour les OIV ou au référencement par une fédération professionnelle représentative du secteur.

Lors des débats sur la loi de programmation militaire (LPM), des engagements avaient été pris au banc mais depuis, le corpus de l'Anssi a changé. L'amendement propose de revenir à ces engagements sur les sondes.

M. Aurélien Lopez-Liguori (RN). L'encadrement par le texte de l'usage de systèmes de détection pour identifier les cyberattaques – les fameuses boîtes noires – est insuffisant. Or ces systèmes ont une grande importance stratégique. Ils captent des flux, détectent des signaux faibles et peuvent être exploités par des puissances étrangères si on n'y prend pas garde. Lors de la LPM, nous avions adopté des mesures prévoyant des qualifications spécifiques pour ces boîtes et interdisant qu'elles soient soumises à des extraterritorialités.

Des entreprises françaises se sont positionnées pour répondre à ces marchés, mais, en raison de la nouvelle politique de l'Anssi, elles font face à une insécurité juridique.

Nous proposons donc de fixer des exigences : qualifications par l'Anssi, obtention d'un visa de sécurité et recours prioritaire à des solutions européennes. Ce sont des garanties à la fois pour notre souveraineté, mais aussi pour ces entreprises qui ont déjà investi beaucoup d'argent dans des solutions souveraines.

Mme Anne Le Hénanff, rapporteure. Ces amendements ne transposent pas la directive et imposent une lourdeur significative aux entités concernées, singulièrement les plus petites d'entre elles.

La logique de NIS 2 n'est pas d'imposer les meilleurs standards dès le début, mais au contraire d'adopter une démarche d'accompagnement progressif.

Avis défavorable.

M. le président Philippe Latombe. Ce point fait l'objet de remontées régulières de l'ensemble des entités, pas seulement des entreprises qui fabriquent des sondes mais également des OIV. Ce qui avait été annoncé dans le cadre de la LPM n'a pas été mis en place. Il nous faudra traiter de ce sujet.

M. Aurélien Lopez-Liguori (RN). La présence de sondes au cœur de nos réseaux peut créer un risque d'ingérence étrangère. Ne pas en parler dans un texte sur la cybersécurité pose problème.

De plus, nous avions voté des dispositions sur les sondes dans la LPM et des engagements forts avaient été pris. L'Anssi est en train de faire marche arrière. Il nous revient de prendre une décision et je pense que ce texte est le bon véhicule.

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

*Puis elle **adopte** successivement les amendements rédactionnels CS355 et CS356 de Mme Anne Le Hénanff, rapporteure.*

Amendements CS222 et CS223 de M. Aurélien Lopez-Liguori (discussion commune)

M. Aurélien Lopez-Liguori (RN). Le projet de loi permet à l'Anssi de confier des audits stratégiques à des organismes indépendants. Or confier de tels audits à des sociétés extra-européennes, c'est prendre le risque d'exposer nos vulnérabilités à des puissances d'où sont originaires ces entreprises.

La direction générale de la sécurité intérieure (DGSI) a rapporté le cas d'entreprises étrangères qui, au cours d'audits dans des entreprises françaises, ont capté des données et des informations. Les plus grands cabinets d'audit, dits Big Four, tous anglo-saxons, réalisent des audits d'entreprises françaises et il arrive de manière assez fréquente qu'une OPA – offre publique d'achat – agressive soit déclenchée dans les semaines ou les mois qui suivent ces audits. Le problème se pose dans les mêmes termes dans le secteur de la cybersécurité.

Nous proposons donc que les organismes qui feront ces audits aient leur « siège statutaire, administration centrale et principal établissement » en France ou dans l'Union européenne.

Mme Anne Le Hénanff, rapporteure. Ces sociétés doivent être certifiées par l'Anssi. On ne peut pas la soupçonner de mettre en péril la sécurité des 15 000 entités françaises qui seront auditées. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). Je ne mets pas en doute les compétences de l'Anssi pour repérer les failles, mais nous ne lui donnons par les armes pour qu'elle traite de l'extraterritorialité et puisse répondre aux ingérences. Nous sommes déjà incapables, ici, de définir la souveraineté numérique ou de définir des règles de la commande publique qui soient protectrices. Or l'Anssi est une autorité qui applique les lois que nous votons. Votre argument me semble donc un peu court.

M. Éric Bothorel, rapporteur général. Imposer un critère de rattachement au seul territoire national pour les organismes indépendants pouvant réaliser des audits serait contraire au principe de la liberté de prestation de services consacré par le Traité sur le fonctionnement de l'Union européenne. Je sais bien que vous voudriez vous passer de nombreux traités européens, mais celui-là est encore en vigueur.

Par ailleurs, l'objectif de protection des informations est déjà satisfait. Celles issues des audits des OIV sont classifiées : elles sont soumises au régime de la protection du secret de la défense nationale, dans le cadre de l'IGI (instruction générale interministérielle) 1300, qui impose notamment une procédure d'habilitation pour les auditeurs. Le code de la défense, qui permet d'externaliser les audits des OIV, ne prévoit en revanche aucune restriction en matière de nationalité.

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

Amendement CS354 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement a pour objectif de garantir que la promotion de solutions de cybersécurité certifiées, prévue par l'article 16, ne crée pas d'effets pervers en défavorisant l'écosystème français et européen de l'innovation, notamment les acteurs du logiciel libre et les PME.

Il s'agit, d'abord, de s'assurer que l'évaluation est fondée sur le mérite technique. Les critères doivent être objectifs et fondés uniquement sur la robustesse et la sécurité de la solution, indépendamment du modèle économique – logiciel libre ou propriétaire – ou de la taille du fournisseur.

Il faut également veiller à ce que les barrières à l'entrée soient réduites. Les modalités prévues ne doivent pas constituer un obstacle insurmontable pour les PME ou des structures, telles que les associations et les fondations, qui développent de nombreux projets de logiciels libres, en cohérence avec l'esprit de l'article 16 de la loi pour une République numérique.

Par ailleurs, notre souveraineté numérique doit être renforcée. En garantissant une compétition équitable, nous permettrons aux solutions françaises et européennes les plus performantes, y compris celles issues du logiciel libre, d'obtenir les qualifications nécessaires pour être déployées dans nos infrastructures critiques, ce qui renforcera notre filière technologique.

Mme Anne Le Hénanff, rapporteure. Je sais que cette question est très importante pour vous. Malheureusement, l'amendement surtransposerait la directive NIS 2. Je dois donc émettre un avis défavorable – je suis navrée de le faire aussi souvent.

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

Amendements identiques CS357 de M. Philippe Latombe et CS238 de M. Aurélien Lopez-Liguori

M. le président Philippe Latombe. Nous devons garantir le maintien des exigences en matière de sécurité et de confiance pour les systèmes et prestataires de détection des incidents de sécurité concernant les opérateurs d'importance vitale – cet amendement porte, de nouveau, sur les sondes. Il s'agit de revenir aux dispositions prévues dans la LPM, sur lesquelles nous avions obtenu, au banc, des engagements du ministre du numérique de l'époque, mais qui ne sont plus suivies par l'Anssi. Cette question n'est pas directement liée au projet de loi, puisqu'elle ne figure pas dans la directive, mais les sondes sont des éléments très importants en matière de cybersécurité. Elles permettent en effet de détecter les intrusions, les fuites de données ainsi que d'autres problèmes.

Mme Anne Le Hénanff, rapporteure. Cet amendement surtransposerait aussi la directive NIS 2 et introduirait vraiment une lourdeur importante. Avis défavorable.

M. le président Philippe Latombe. Il existe un véritable problème en ce qui concerne les sondes, pas simplement pour leurs fabricants européens ou français, mais aussi et surtout pour les OIV, d'abord parce qu'ils ont subi un changement de corpus imposé par l'Anssi depuis quelques mois, et ensuite parce que la présence éventuelle de sondes d'origine extraterritoriale dans leurs systèmes d'information pose des questions en matière de cybersécurité et d'ingérence. Il faudra trouver un véhicule pour régler ce problème : si ce n'est pas ce texte, le gouvernement devra prendre, au banc, l'engagement que le sujet sera traité.

M. Aurélien Lopez-Liguori (RN). C'est une question de sécurité nationale. Si les niveaux de qualification pour les sondes, qui se trouvent au tout début de la chaîne de détection, ne sont pas les bons, ce qui risque de se traduire par une non-efficience, et que nous sommes exposés à des ingérences, la situation devient problématique. Ces amendements conduiraient peut-être à une surtransposition et ce n'est pas peut-être le bon lieu pour les examiner, mais il est urgent d'agir. Il n'y a pas d'autre texte disponible ; sauf si vous nous promettez de présenter un texte portant sur les sondes ou une nouvelle LPM dans les prochains mois, nous risquons d'être confrontés à des problèmes de sécurité nationale dans les semaines, les mois ou les années à venir.

M. Éric Bothorel, rapporteur général. Cette question est effectivement importante, mais elle n'a pas sa place dans le présent texte, pour une raison de surtransposition à laquelle nous sommes tous sensibles. Comme nous ne pouvons pas davantage être aveugles ou sourds à ce qui remonte des écosystèmes, le mieux serait d'appeler l'attention du prochain gouvernement, dès qu'il sera nommé, en particulier du ministre chargé de ces questions, sur la nécessité de trouver ensemble les voies et moyens d'une solution dans le cadre du présent texte ou de retrouver dans un texte ultérieur une traduction des engagements pris à l'occasion de la LPM. Nous ne pouvons pas laisser en l'état les éléments actuels, car ce ne serait efficace ni pour notre écosystème ni pour les utilisateurs de ces outils. L'engagement que je prends, en tant que rapporteur général, est d'y travailler dès que nous aurons un ou une ministre. Cela fera partie des points que nous devrons faire remonter et traiter ensemble.

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

*Elle **adopte** l'article 16 **modifié**.*

Article 16 *bis* : *Empêcher l'intégration de dispositifs techniques visant à affaiblir la sécurité des systèmes d'information et des communications électroniques*

Amendement CS494 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Cette partie du projet de loi, attendue par beaucoup, nous fait revenir sur des débats que nous avons déjà eus dans l'hémicycle au sujet d'un autre texte.

Mon amendement tend à réécrire l'article 16 *bis*, introduit par le Sénat. Politiquement, la question a été purgée, si je puis dire, puisque l'article 8 *ter* de la proposition de loi visant à sortir la France du piège du narcotrafic n'a finalement pas été retenu. L'Assemblée nationale a tranché en faveur du maintien du chiffrement de bout en bout : elle n'a pas accepté des dispositions de nature à l'affaiblir. Le Sénat a eu des regrets, au point d'utiliser désormais un autre véhicule législatif pour introduire une mesure orthogonale par rapport à celle qu'il avait adoptée en première intention.

Vous connaissez mon combat, de longue date, pour la protection du chiffrement de bout en bout. Je n'ai pas attendu le texte sur le narcotrafic ou celui que nous sommes en train d'examiner pour défendre en public la nécessité de consacrer pleinement le droit au chiffrement de bout en bout, auquel tous les outils de messagerie ont recours. Il est quasiment devenu un standard, et c'est tant mieux parce que cela protège nos échanges. Dans le temps, on protégeait les conversations et les courriers, et il en est de même, d'une manière encore plus efficace, pour les messageries actuelles.

Pour autant, je crois que nous ne pouvons pas en rester à la rédaction proposée par le Sénat. Il est assez baroque d'écrire qu'il faut, pour consacrer un droit, prendre des dispositions afin d'éviter qu'il disparaisse. Je connais peu de cas, dans notre droit, où l'on raisonne ainsi. En l'état, la rédaction est donc perfectible. Je propose de commencer par rappeler que le chiffrement présente un intérêt général majeur. Par ailleurs, si la question politique est derrière nous, un sujet technique reste en suspens. Un certain nombre d'acteurs qui procèdent à des enquêtes nous disent qu'ils font face à des difficultés et qu'il pourrait être nécessaire de se réinterroger demain sur les méthodes et les moyens d'aujourd'hui. Si nous gardions la rédaction adoptée par le Sénat, nous empêcherions les réflexions techniques en cours, qui demandent du temps.

Je fais partie de ceux qui trouvent que le chiffrement de bout en bout est sacré, mais pas suffisamment pour qu'on écarte l'idée que des experts, des spécialistes sur le plan technique, puissent se demander comment préserver le dispositif actuel, pour assurer la protection du plus grand nombre, tout en parvenant, sans altérer les principes, à obtenir des informations sur ceux qui nous nuisent. C'est une telle articulation que je vous propose. Il est important, dans le moment que nous vivons, de ne pas voter à la légère des dispositions qui empêcheraient d'aller plus loin dans les nécessaires réflexions techniques qui sont actuellement menées.

Mme Anne Le Hénanff, rapporteure. Nous arrivons donc au tant attendu article 16 *bis*.

J'aurais donné un avis défavorable à l'amendement de suppression de l'article de M. Mazaury si notre collègue avait été là pour le défendre.

Nous avons auditionné les services de renseignement. Ils plébiscitent la possibilité qui pourrait leur être donnée d'utiliser certaines techniques ou en tout cas de se renseigner sur ce point. C'était un moment important : ils ont pu nous expliquer tranquillement leur point de vue. Nous avons également auditionné les industriels, qui ne sont pas favorables, quant à eux, à une telle évolution. Ils estiment, nous ont-ils dit, que cela introduirait une faille dans leurs systèmes, ce qu'ils refusent catégoriquement.

Le président de la commission des lois a créé un groupe de réflexion sur cette thématique, à la suite du psychodrame lié à la proposition de loi dite « narcotrafic ». Le secrétariat général de la défense et de la sécurité nationale (SGDSN) et la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) nous ont indiqué qu'ils ont créé un groupe de travail pour identifier des solutions techniques. Ce que vous proposez, monsieur le rapporteur général, c'est de donner une chance à ce travail d'avancer. Je ne suis donc favorable ni à la suppression de l'article 16 *bis* ni au maintien de sa rédaction actuelle, qui n'est pas complète, est assez fermée et nous contraindrait pour les mois et les années à venir, alors que la menace n'a jamais été aussi prégnante, mais je suis favorable à l'amendement du rapporteur général.

M. le président Philippe Latombe. L'adoption de cet amendement de réécriture ferait tomber les suivants. Comme le sujet a, par ailleurs, fait l'objet de longues discussions lors de l'examen de la proposition de loi concernant le narcotrafic, je propose aux groupes qui le souhaitent de s'exprimer.

M. Denis Masséglia (EPR). Cette question est ô combien importante, puisqu'il s'agit, d'une part, d'assurer la liberté individuelle, qui justifie l'absence d'accessibilité aux échanges grâce à certains outils et, d'autre part, de donner aux enquêteurs la possibilité de faire leur travail. La proposition du rapporteur général est conforme à notre exigence de sécurité et de nature à donner aux enquêteurs la capacité de trouver les personnes qui ne respectent pas la législation. Le groupe Ensemble pour la République est farouchement favorable à la proposition équilibrée qui nous est soumise.

M. Arnaud Saint-Martin (LFI-NFP). Cet amendement de réécriture affaiblirait la portée originelle de l'article 16 *bis*, qui, même s'il n'est peut-être pas parfait du point de vue rédactionnel, va dans le bon sens en étant « fermé », comme l'a dit la rapporteure. Il prend acte de la fin programmable des messageries cryptées si l'on remet en cause leur chiffrement de bout en bout, donc leur mode de fonctionnement, ce qui serait antidémocratique et contraire aux libertés individuelles.

Comme l'avait dit le groupe Insoumis lors de l'examen de la proposition de loi portant sur le narcotrafic, qui a fait l'objet de nombreuses discussions, casser un protocole de chiffrement ou le contourner pose exactement les mêmes problèmes. Le service est contraint de modifier son code et son algorithme ; la vulnérabilité qui est créée peut être utilisée par d'autres acteurs potentiellement malveillants ; cette évolution peut ensuite être étendue à d'autres finalités ; on affaiblit la sécurité générale des infrastructures de réseau, au détriment de tous les utilisateurs.

Nous défendons un renseignement tourné vers les moyens humains, qui manquent, hélas, mais ont fait leurs preuves, et nous pensons qu'il faut assurer la continuité des services chiffrés de bout en bout. Je voterai donc contre cette réécriture au nom du groupe Insoumis, certes un peu seul dans cette salle mais en conscience.

Mme Marie Récalde (SOC). Les arguments du rapporteur général et de la rapporteure peuvent s'entendre, mais nous sommes très attachés aux libertés individuelles, auxquelles nous considérons qu'une atteinte serait portée. Comme vous l'avez dit, monsieur le rapporteur général, le chiffrement est sacré. Nous voterons donc contre cet amendement.

Mme Catherine Hervieu (EcoS). Une lutte historique s'est engagée, depuis les révélations d'Edward Snowden, contre l'installation de *backdoors* – portes dérobées – sur nos téléphones portables. Il faut aussi que le chiffrement reste un droit fondamental. Tout ce qui pourrait contribuer à le fragiliser ou à l'affaiblir doit être évité. Dans sa rédaction actuelle, l'article 16 *bis* est un symbole fort, qui montre que nous avons bien tiré les leçons de la surveillance de masse et du capitalisme de surveillance. Nous voterons donc contre l'amendement du rapporteur général.

M. Aurélien Lopez-Liguori (RN). Nous irons dans le même sens que les derniers orateurs. Le chiffrement de bout en bout est un droit et une nécessité. Nous avons expliqué notre position lors des débats sur la proposition de loi concernant le narcotrafic. Il n'y a pas d'autre solution, à l'heure actuelle, qu'un abaissement du niveau de chiffrement pour intercepter les messages. D'autres solutions existeront peut-être dans cinq ou dix ans, mais nous pourrons alors réécrire la loi. Nous n'avons pas totalement confiance dans la manière dont de prochains gouvernements pourraient utiliser un affaiblissement de l'article 16 *bis*, que le Sénat a voulu, dans sa grande sagesse, introduire dans le texte.

Mme Marina Ferrari (Dem). Contrairement au rapporteur général, je crains que le débat politique ne soit pas clos, mais c'est précisément pour cette raison que j'irai dans le même sens que lui. Nous sommes tiraillés entre l'obligation impérieuse de protéger le chiffrement de bout en bout, pour des raisons touchant à la fois aux libertés individuelles et à la sécurité, car il ne faudrait pas introduire de nouvelles failles, et le fait que dans la lutte pour assurer la sécurité de la population, notamment face à la grande criminalité, il faut bien qu'on puisse mener des investigations sur les possibilités techniques qui pourraient se présenter. La réécriture de l'article 16 *bis* qui nous est proposée est intéressante puisqu'elle nous permettrait d'avoir un échange, peut-être dans le cadre de la navette parlementaire, puis un rapport. Il faudrait veiller à ce que le travail prévu soit effectivement mené et qu'il en sorte un rapport au terme du délai de douze mois, mais l'équilibre proposé par cet amendement mérite d'être exploré.

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

Amendement CS224 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Le présent article, ajouté par les sénateurs, vise à protéger les communications électroniques contre toute tentative d'affaiblissement des dispositifs de sécurité. C'est une nécessité, mais le terme « chiffrement » qui a été retenu est peut-être trop restrictif puisqu'il ne couvre que la confidentialité des échanges. La cybersécurité repose sur un socle beaucoup plus large : l'intégrité des données, l'authentification des utilisateurs et la non-répudiation des échanges, qui relèvent d'un domaine plus global, et reconnu en droit, la cryptographie. Notre amendement vise ainsi à remplacer « chiffrement » par « cryptographie », terme qu'on trouve déjà dans le code de la défense, dans la loi de 2004 pour la confiance dans l'économie numérique et dans le règlement européen sur l'identification électronique dit eIDAS. Nous devons, dans un souci de clarté, utiliser le bon terme.

Mme Anne Le Hénanff, rapporteure. Cette substitution ne me semble pas opportune : le terme « chiffrement » convient davantage. Avis défavorable.

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

Amendement CS358 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement tend à élargir le champ de l'article 16 *bis* pour inclure, au-delà des outils techniques tels que les portes dérobées et les clés maîtresses, certaines pratiques, comme la création d'un accès non consenti aux données protégées et la mise en place d'un protocole de remise systématique de copies des clés privées, qui auraient, *in fine*, le même effet.

Mme Anne Le Hénanff, rapporteure. Cette précision est très utile. Au-delà des outils techniques, il faut prendre en considération la question des pratiques. Avis favorable.

M. Éric Bothorel, rapporteur général. Défavorable.

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

M. Paul Midy (EPR). Il est important de protéger la vie privée, mais aussi la vie en général, en donnant à nos services de sécurité les moyens de faire leur job. Je pense qu'il est nécessaire et possible de faire les deux. La rédaction proposée par le rapporteur général était très bonne : elle permettrait d'avancer sur ce sujet, en trouvant les moyens à utiliser. Il faut donc continuer le travail, car rien ne paraît définitif dans cette assemblée.

La commission ***adopte*** *l'article 16* bis ***modifié****.*

Article 17 : *Obligation de notification à l'ANSSI des incidents importants*

La commission ***adopte*** *l'amendement rédactionnel CS359 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS362 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Les alinéas 3 et 4 de l'article 17 prévoient que chaque incident, qu'il ait causé ou non une perturbation opérationnelle ou des dommages matériels, corporels ou moraux, fait l'objet d'une notification à l'Anssi. Si la volonté de couvrir l'ensemble des incidents importants peut tout à fait s'entendre, les modalités de leur prise en compte restent éloignées des réalités rencontrées sur le terrain par les entités importantes ou essentielles en cas de crise cyber. Les incidents déclenchent automatiquement une réponse opérationnelle, conformément aux procédures internes en vigueur, dont la priorité est le rétablissement du service. Faute d'être en mesure d'apprécier précisément l'impact opérationnel d'un incident à l'aide d'une méthodologie adaptée, les entités concernées ne sont pas capables de savoir si ce dernier est susceptible d'entrer dans la catégorie des incidents importants ni d'anticiper d'éventuelles conséquences ou dommages pour les tiers. En ce sens, la rédaction des alinéas 3 et 4 est trop large, manque de proportionnalité et fait peser un risque juridique sur les entités régulées. Il conviendrait plutôt de cantonner les notifications aux incidents pour lesquels l'impact opérationnel est incontestable.

M. Éric Bothorel, rapporteur général. Les alinéas 3 et 4 de l'article 17 reprennent strictement la définition prévue à l'article 23 de la directive NIS 2. Le changement proposé, qui réduirait le champ des incidents notifiés à l'Anssi, constituerait une sous-transposition de la directive. Il est en outre primordial que l'Anssi ait une vision aussi complète que possible de la menace. Avis défavorable.

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

Amendement CS361 de M. Philippe Latombe

M. le président Philippe Latombe. Tout incident entraîne des pertes financières, allant de quelques centaines à plusieurs dizaines de millions d'euros. Il est souhaitable de qualifier ces pertes comme importantes ou significatives, afin de limiter le nombre de déclarations.

Mme Anne Le Hénanff, rapporteure. C'est une précision utile. Avis favorable.

M. Éric Bothorel, rapporteur général. J'ai une autre lecture : cet amendement conduirait à une surtransposition. L'alinéa 3 du présent article reprend strictement ce que demande l'article 23 de la directive. Avis défavorable.

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

Amendement CS363 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement vise à assurer une articulation claire entre le droit national et les exigences européennes en matière de cybersécurité s'agissant de la qualification des incidents importants. Pour les entités exerçant des activités dans les secteurs critiques et hautement critiques définis aux annexes I et II de la directive NIS 2, l'évaluation des incidents doit se faire sur la base du cadre, détaillé et normé, prévu par un règlement d'exécution qui va bien au-delà des critères généraux mentionnés aux alinéas 2 à 4 du présent article et offre une méthodologie claire et harmonisée pour l'ensemble des États membres.

M. Éric Bothorel, rapporteur général. L'amendement est satisfait puisque notre intention est bien de faire référence à ce règlement. Toutefois, en le figeant dans notre droit, nous prendrions le risque de devoir y revenir à la moindre modification du texte, alors qu'aucune ambiguïté n'existe quant à son application. C'est pourquoi je vous invite à le retirer ; à défaut, j'émets un avis défavorable.

Mme Anne Le Hénanff, rapporteure. Je souhaite le maintenir.

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

*Puis elle **adopte** l'amendement rédactionnel CS365 de Mme Anne Le Hénanff, rapporteure.*

*L'amendement CS225 de M. Aurélien Lopez-Liguori est **retiré**.*

Amendement CS153 de Mme Marina Ferrari

Mme Marina Ferrari (Dem). Il vise à préciser que la notification est adressée à l'Anssi.

Mme Anne Le Hénanff, rapporteure. J'y suis défavorable car la notification ne se fait pas à l'Anssi mais aux entités. J'ai d'ailleurs déposé un amendement en ce sens.

M. Éric Bothorel, rapporteur général. Votre amendement ne permet pas de transposer de manière satisfaisante l'article 23 de la directive NIS 2, qui prévoit que les incidents importants et les vulnérabilités critiques visés aux alinéas 14 et 15 soient notifiés par les entités assujetties aux destinataires de leurs services et non à l'autorité nationale. Il y a donc une erreur de compréhension de la logique de l'article. C'est pourquoi je vous invite à retirer votre amendement ; à défaut, j'émets un avis défavorable.

En revanche, vous avez identifié un point d'ambiguïté qui gagnerait à être corrigé soit par un amendement de la rapporteure, soit en séance, afin de clarifier le texte.

*L'amendement est **retiré**.*

Amendements identiques CS496 de M. Éric Bothorel et CS368 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Mon amendement vise à reprendre la rédaction du point 2 de l'article 23 de la directive NIS 2 qui régit les obligations des États membres et des entités en matière d'information aux destinataires des services lorsque l'entité essentielle ou importante constate qu'une vulnérabilité critique est susceptible de les affecter.

L'objectif est de clarifier les informations devant leur être communiquées en s'alignant sur le point 2 de l'article précité, qui en limite le champ aux mesures et aux corrections que ces destinataires peuvent appliquer et, le cas échéant, aux informations relatives à la vulnérabilité elle-même.

L'amendement vise également à préciser la rédaction du texte actuel qui n'indique pas à qui sont notifiés les incidents importants et les vulnérabilités critiques.

M. le président Philippe Latombe. Je précise que si ces amendements sont adoptés, ils feront tomber les trois amendements identiques suivants. Leurs auteurs souhaitent-ils prendre la parole ?

Mme Sabine Thillaye (Dem). Mon amendement vise à harmoniser la directive et la loi de transposition en matière de vulnérabilité, en substituant au terme « critique » le mot « importante ».

M. Denis Masséglia (EPR). L'objectif est de rester le plus proche possible du texte de base : mieux vaut éviter les surtranspositions, qui mettent toujours en difficulté les personnes concernées.

M. le président Philippe Latombe. J'ai en effet déposé l'amendement CS370 car je considère que la rédaction actuelle s'apparente à une surtransposition ; il me semble préférable de rester fidèle à la directive.

*La commission **adopte** les amendements identiques CS496 et CS368.*

*En conséquence, les amendements identiques CS370, CS21 et CS35 **tombent**.*

*La commission **adopte** les amendements rédactionnels CS371 et CS372 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS373 de M. Philippe Labombe

M. le président Philippe Latombe. Comme le souligne l'alinéa 14, un incident important peut avoir des conséquences graves, ce qui justifie que les autorités compétentes du secteur d'activité concerné, et éventuellement la Commission nationale de l'informatique et des libertés (Cnil), en soient informées, afin de prendre les mesures nécessaires.

Selon le principe « dites-le nous une fois », et afin que l'entité victime de l'incident important se concentre sur son traitement, l'autorité nationale de sécurité des systèmes d'information, première destinataire de la notification, doit en assurer la transmission aux administrations ou aux autorités concernées. L'entité victime sera réputée avoir rempli les obligations légales de notification propres à son activité en communiquant l'incident à un guichet unique, opéré par l'autorité nationale de sécurité des systèmes d'information.

Comme cela a été évoqué à de nombreuses reprises lors des auditions, il s'agit de disposer d'un guichet unique qui permette aux entités soumises à la fois à NIS 2, au règlement sur la résilience opérationnelle numérique du secteur financier, dit Dora, et à l'obligation de déclaration à la Cnil dans le cadre des pertes de données personnelles, de disposer d'un seul formulaire de déclaration qui soit adressé à l'ensemble des autorités compétentes.

Mme Anne Le Hénanff, rapporteure. Je comprends l'idée, mais je ne pense pas que la rédaction retenue soit satisfaisante. Ce sujet important mérite que nous y travaillons encore, en vue de la séance publique. Avis défavorable.

M. le président Philippe Latombe. Je comprends votre intention d'y réfléchir de façon plus approfondie. Cependant, si nous n'acceptons aucune modification dans le cadre de la commission, nous n'aurons pas forcément l'occasion d'y revenir en séance. C'est pourquoi, même si sa rédaction vous semble imparfaite, je souhaite maintenir mon amendement pour inscrire dans la loi le principe du guichet unique, en espérant que nous disposerons, d'ici à la séance, de l'expertise des services sur ce sujet. Ce faisant, nous aurons au moins répondu aux nombreuses demandes exprimées lors des auditions.

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

*La commission **adopte** les amendements rédactionnels CS374 et CS375 de Mme Anne Le Hénanff, rapporteure.*

*La commission **adopte** l'article 17 **modifié**.*

La réunion est suspendue de vingt-trois heures cinq à vingt-trois heures dix.

Section 3
Enregistrement des noms de domaine

Article 18 : *Détermination des critères territoriaux pour l'application aux offices et aux bureaux d'enregistrement des noms de domaine*

*La commission **adopte** l'amendement rédactionnel CS376 de Mme Anne Le Hénanff, rapporteure.*

*Puis, elle **adopte** l'article 18 **modifié**.*

Article 19 : *Obligation pour les offices et les bureaux d'enregistrement des noms de domaine de mettre en place une base de données*

Amendements identiques CS476 de M. Éric Bothorel, CS80 de M. Denis Masséglia, CS111 de M. René Pilato et CS188 de Mme Marie Récalde

M. Denis Masséglia (EPR). L'amendement vise, une fois de plus, à garantir la transposition effective de la directive NIS 2.

M. Arnaud Saint-Martin (LFI-NFP). Notre amendement permet de s'assurer que l'ensemble des informations relatives au titulaire du nom de domaine sont effectivement collectées par les bureaux et les offices d'enregistrement, même lorsque celui-ci recourt à des services tiers pour effectuer ses démarches.

En effet, certains titulaires ont recours à des services pour anonymiser leurs données, ce qui rend plus difficile, voire impossible, d'intenter des actions en justice contre eux le cas échéant. De nombreux acteurs dont les droits pourraient être bafoués par des entités numériques peu scrupuleuses – je pense aux droits d'auteur, aux droits des consommateurs – seraient ainsi privés du droit à un recours effectif. Cet amendement, élaboré en collaboration avec la Société civile des producteurs phonographiques (SCPP), vise à éviter ces situations, d'autant plus que l'article 28 de la directive NIS 2 prévoit la collecte des informations « du point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire ».

Mme Anne Le Hénanff, rapporteure. Ces amendements identiques semblent relever du domaine réglementaire. Néanmoins, je m'en remets à la sagesse de la commission.

M. Éric Bothorel, rapporteur général. J'y suis, pour ma part, très favorable.

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

Amendements identiques CS497 de M. Éric Bothorel et CS377 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Le projet de loi emploie, en lieu et place des termes « entités fournissant des services d'enregistrement de noms de domaine » utilisés dans la directive, ceux de « bureaux d'enregistrement » utilisés dans le code des postes et des communications électroniques. Cet amendement vise donc, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations en matière de protection des données prévues à l'alinéa 2 de l'article 19 du projet de loi.

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

*L'amendement CS498 de M. Éric Bothorel, rapporteur général, est **retiré**.*

Amendements identiques CS102 de M. Antoine Villedieu et CS378 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il vise à clarifier le fait que les procédures de vérification des données n'ont pas pour objectif de s'assurer de leur exactitude au moment de leur collecte. En effet, les offices et les bureaux d'enregistrement n'ont pas les capacités d'effectuer une telle vérification au moment même de la collecte pour l'ensemble des noms de domaine. Cette précision a été demandée par les acteurs du domaine lors des auditions.

M. Éric Bothorel, rapporteur général. Sagesse.

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

Amendements identiques CS81 de M. Denis Masséglia et CS112 de M. René Pilato

M. Denis Masséglia (EPR). Cet amendement vise à préciser la liste des données relatives à l'enregistrement des noms de domaine devant être récupérées par les bureaux et les offices d'enregistrement dans le cadre de leur mission. Cette liste doit reprendre, au minimum, les données mentionnées au point 2 de l'article 28 de la directive NIS 2, en y ajoutant les adresses postales des titulaires et des points de contact du nom de domaine.

À défaut, le décret d'application devra indiquer la nécessité de collecter l'adresse postale des titulaires et des points de contact.

Mme Anne Le Hénanff, rapporteure. Comme précédemment, il me semble que ces amendements relèvent du domaine réglementaire. Sagesse.

M. Éric Bothorel, rapporteur général. La liste des données collectées par les offices et les bureaux d'enregistrement, ainsi que par les agents agissant pour le compte de ces derniers, ne relève pas du domaine de la loi, conformément à l'article 34 de la Constitution. Ces données seront précisées au niveau réglementaire. Avis défavorable.

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

*Puis elle **adopte** l'amendement rédactionnel CS379 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS82 de M. Denis Masséglia et CS113 de M. René Pilato

M. Denis Masséglia (EPR). Cet amendement important vise à spécifier le contenu du décret afférent à l'article 19, qui devra préciser les procédures de vérification des données d'enregistrement des noms de domaine menées par les bureaux et les offices d'enregistrement.

M. Arnaud Saint-Martin (LFI-NFP). Élaboré en collaboration avec la SCPP, notre amendement vise à préciser les conditions d'enregistrement des noms de domaine par les offices et les bureaux d'enregistrement qui seront fixées, en vertu de l'article 19, par un décret qui précisera la liste des données devant être collectées. L'objectif est de garantir l'application de l'article 28 de la directive NIS 2, en imposant que le décret prévoie aussi les procédures de vérification. En effet, afin de mieux garantir la traçabilité des titulaires des noms de domaine, la directive NIS 2 propose aux pays membres de mettre en œuvre des procédures de vérification, pour corriger, d'une part, les données inexactes et pour faciliter, d'autre part, la transparence.

Mme Anne Le Hénanff, rapporteure. Avis défavorable.

M. Éric Bothorel, rapporteur général. Le point 3 de l'article 28 de la directive dispose que les États membres exigent que les offices, les bureaux et les agents agissant pour les bureaux, aient mis en place des politiques et des procédures, notamment des procédures de vérification des données d'enregistrement. Dès lors, détailler au niveau réglementaire les modalités de vérification des données collectées, alors même que la directive ne prévoit aucune modalité précise et laisse le soin aux entités de les définir, présenterait un risque élevé de mauvaise transposition. Pour cette raison, je suis défavorable aux amendements.

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

*Puis elle **adopte** l'article 19 **modifié**.*

Article 20 : *Durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaine*

Amendements identiques CS499 de M. Éric Bothorel et CS380 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Le projet de loi emploie, en lieu et place des termes « entités fournissant des services d'enregistrement de noms de domaine » utilisés dans la directive, ceux de « bureaux d'enregistrement » utilisés dans le code des postes et des communications électroniques. Cet amendement vise, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations prévues à l'article 20 du projet de loi portant sur la durée de conservation des données relatives à chaque nom de domaine.

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

Amendement CS56 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Cet amendement vise à protéger les données collectées en sécurisant leur sauvegarde et en limitant leur usage aux seuls besoins spécifiques des procédures pénales et des enquêtes en cybersécurité. La conservation étendue des données permet d'éviter que des preuves essentielles soient détruites prématurément, ce qui pourrait compromettre la poursuite des infractions graves liées au cybercrime ou à d'autres formes de délinquance numérique.

Mme Anne Le Hénanff, rapporteure. La durée de sauvegarde de dix ans me paraît excessive. Par ailleurs, cette disposition surtranspose la directive NIS 2. Avis défavorable.

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

*Puis elle **adopte** l'article 20 **modifié**.*

Article 21 : *Obligation de publication des données d'enregistrement d'un nom de domaine*

Amendements identiques CS500 de M. Éric Bothorel et CS381 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Comme pour l'amendement CS380, cet amendement vise, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement l'obligation de publication des données d'enregistrement qui n'ont pas de caractère personnel, prévue à l'article 21 du projet de loi.

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

*Puis elle **adopte** l'article 21 **modifié**.*

Article 22 : *Obligation de communiquer les données collectées par les offices et les bureaux d'enregistrement à l'autorité judiciaire et à l'ANSSI pour les besoins des procédures pénales ou de la sécurité des systèmes d'information*

Amendement CS383 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Le présent amendement élargit le champ des demandeurs d'accès légitimes aux agents assermentés expressément habilités par la loi, notamment en matière de propriété intellectuelle, de protection de l'enfance ou des consommateurs, ainsi qu'aux commissaires de justice, en plus de l'Anssi et des forces publiques d'enquête. Cette clarification sécurise les conditions d'accès, aligne le droit national sur le cadre européen et garantit l'effectivité du droit d'accès aux données des noms de domaine pour lutter contre les usages frauduleux ou illicites, sans imposer de charge disproportionnée aux offices d'enregistrement.

M. Éric Bothorel, rapporteur général. L'amendement tel qu'il est rédigé élargit le champ des demandeurs d'accès à toute personne habilitée par la loi et fait donc peser un risque d'élargissement inconsidéré, sans besoins identifiés. J'ajoute que la demande initiale sera satisfaite par les amendements identiques CS12, CS15, CS88 et CS168, qui seront examinés ultérieurement, en ce qui concerne la lutte contre la contrefaçon. Demande de retrait ou, à défaut, avis défavorable.

L'amendement est ***retiré****.*

La commission ***adopte*** *l'amendement rédactionnel CS382 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS501 de M. Éric Bothorel et CS384 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Comme précédemment, l'amendement vise à appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations prévues à l'article 22 du projet de loi.

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

Amendement CS88 de M. Denis Masséglia

Mme Anne Le Hénanff, rapporteure. Cet amendement me semble surtransposer la directive. Néanmoins, dans le doute, je m'en remets à la sagesse de la commission.

M. Éric Bothorel, rapporteur général. Lors de l'examen de l'amendement CS383 de la rapporteure, j'ai répondu que les propositions formulées par cet amendement étaient de nature à lutter efficacement contre les contrefaçons. Je confirme donc ma position et émets un avis favorable.

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

Puis elle ***adopte*** *les amendements rédactionnels CS385 et CS386 de Mme Anne Le Hénanff, rapporteure.*

*La commission **adopte** l'article 22 **modifié**.*

Section 4
Coopération et échanges d'informations

Article 23 : *Dérogation aux secrets protégés par la loi pour la communication d'informations en matière de cybersécurité entre l'ANSSI et ses interlocuteurs*

*La commission **adopte** l'amendement rédactionnel CS387 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS227 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Cet amendement répond également aux interrogations de Mme Le Hénanff. En effet, le texte prévoit de protéger les intérêts commerciaux des entités lors des échanges d'informations avec l'Anssi. Toutefois, cette notion d'intérêts commerciaux est floue et juridiquement fragile. C'est pourquoi nous proposons de la remplacer par « les secrets protégés par la loi », ce qui recouvrira les secrets des affaires, les secrets industriels ou commerciaux et ceux liés à la défense nationale, notion juridique plus solide, reconnue et déjà encadrée par la loi.

Mme Anne Le Hénanff, rapporteure. Je partage votre analyse. Cependant, je vous propose de retirer votre amendement au profit du mien, le CS388, qui me semble plus équilibré, puisqu'il supprime la mention des intérêts commerciaux.

M. Éric Bothorel, rapporteur général. J'en demande également le retrait parce que la référence aux secrets protégés par la loi irait à l'encontre des objectifs recherchés par les échanges d'informations autorisés par ce même article et serait contraire aux dispositions de son premier alinéa. Par conséquent, l'amendement rendrait ces dispositions inopérantes.

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

Amendement CS388 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Sur le même sujet, cet amendement est destiné à éviter l'introduction d'une notion dont les contours ne sont pas déterminés en droit français, lequel connaît en revanche celle de secret des affaires. L'objectif étant que le partage d'informations puisse avoir lieu entre les autorités compétentes s'il est nécessaire à l'exercice des missions qui leur sont confiées par les textes, les garanties de confidentialité et de partage limité à ce qui est justifié figurent dans le texte et sont de nature à répondre aux prescriptions de la directive NIS 2.

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

Amendement CS228 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Les échanges d'information entre l'Anssi, la Cnil, la Commission européenne ou les CSIRT – centres de réponse aux incidents de sécurité

informatique – concernent de nouvelles données, ultrasensibles, qui ne doivent pas transiter par des solutions soumises à des règles extraterritoriales. Or nous ne disposons pas encore de solutions permettant d'effectuer de tels échanges. C'est pourquoi il est nécessaire de préciser dans la loi qu'ils doivent être effectués dans des conditions garantissant l'immunité face aux lois extraterritoriales.

Mme Anne Le Hénanff, rapporteure. Avis défavorable puisqu'il s'agit d'une surtransposition.

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

*Puis elle **adopte** l'article 23 **modifié**.*

Article 24 : *Agrément par l'ANSSI d'organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents cyber*

*La commission **adopte** l'amendement rédactionnel CS389 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS55 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Cet amendement vise à s'assurer que les échanges d'informations couvertes par le secret soient limités au strict minimum et proportionnés à l'objectif du partage, afin d'assurer la meilleure protection possible des données qui en relèvent.

Cette précision légistique – qui reprend des dispositions déjà intégrées par voie d'amendement au Sénat à l'article 23 – est d'autant plus nécessaire que nous assistons depuis de nombreuses années à une fragilisation de certains secrets protégés par la loi, comme celui de l'instruction, au nom d'un intérêt supposé supérieur qui justifierait de déroger aux principes les plus fondamentaux – dans le cas présent, la lutte contre la cybermenace. Dans ce contexte, et puisque le paragraphe 13 de la directive NIS 2 prévoit une dérogation aux secrets protégés par la législation nationale dès lors que l'échange d'informations est nécessaire à l'application de la directive, nous souhaitons encadrer au maximum cette possibilité en prévoyant que l'échange soit limité au strict nécessaire et proportionné au but recherché.

Mme Anne Le Hénanff, rapporteure. Votre amendement me semble déjà satisfait. Néanmoins, je ne m'y oppose pas fondamentalement. Sagesse.

M. Éric Bothorel, rapporteur général. Je suis plus sévère. L'amendement est, en effet, déjà satisfait compte tenu de l'approche proportionnée des dispositions du projet de loi, qui prévoit déjà des garanties tant pour le respect de la législation protégeant le secret que pour les intérêts économiques des entités, par exemple à l'article 17, alinéa 17, ou le secret professionnel auquel les agents et les personnels sont astreints dans les conditions prévues à l'article 226-13 du code pénal, à l'article 27. Il importe que, dans le cadre spécifique de la réponse à un incident, ces dispositions ne soient pas interprétées comme faisant obstacle à la transmission d'informations pourtant nécessaires et proportionnées. Je demande donc le retrait de l'amendement. À défaut, avis défavorable.

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

Amendement CS191 de Mme Marie Récalde

Mme Marie Récalde (SOC). Il vise à prévoir que les relais désignés par l'Anssi, dans le cadre des articles relatifs à l'accompagnement des entités, puissent, sous condition d'agrément, assurer la délivrance du label de confiance attestant de la mise en œuvre par les entités importantes et les entités essentielles mentionnées aux articles 8 et 9 des mesures de sécurité prévues par décret en application de la présente loi, et ayant pour objet de reconnaître le respect effectif des exigences techniques, organisationnelles et opérationnelles permettant d'assurer un niveau élevé de cybersécurité.

Cette disposition pourra notamment permettre aux campus cyber régionaux et aux CSIRT territoriaux qui choisiront l'agrément d'affirmer leur rôle de tiers de confiance dans les territoires, en complément de leurs missions existantes de sensibilisation, de soutien opérationnel et d'accompagnement à la mise en conformité des entités publiques et privées. Ce label deviendra ainsi un outil structurant au service des écosystèmes régionaux de cybersécurité.

Mme Anne Le Hénanff, rapporteure. Il est opportun que le label, même sous condition d'agrément, ne soit pas étendu au-delà de l'Anssi. Par ailleurs, la directive ne prévoit pas cette possibilité. Avis défavorable.

M. Éric Bothorel, rapporteur général. Je profite de cette occasion pour souligner le rôle important des CSIRT et des campus cyber régionaux, dans lesquels nous avons tous des amis et des contacts qui y travaillent au quotidien.

Avis défavorable toutefois. Inscrire dans la loi la possibilité pour les CSIRT relais de délivrer un label de confiance ne semble pas utile, parce que leur mission relève du niveau réglementaire et qu'en l'état, rien ne les empêche de se faire accréditer à cette fin comme organismes de contrôle par le Cofrac.

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

Elle ***adopte*** *l'article 24* ***modifié****.*

Après l'article 24

Amendement CS391 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à transposer les dispositions de l'article 29 de la directive NIS 2, qui prévoit l'existence d'accords de partage d'informations en matière de cybersécurité, permettant aux entités essentielles, aux entités importantes et à leurs prestataires en matière de cybersécurité d'échanger des informations détaillées et opérationnelles sur les menaces cyber, afin de mieux y faire face.

Les considérants 119 et 120 de la directive rappellent l'importance de ce dispositif : « le partage d'informations contribue à accroître la sensibilisation aux cybermenaces, laquelle renforce à son tour la capacité des entités à empêcher les menaces de se concrétiser en incidents réels et leur permet de mieux contenir les effets des incidents et de se rétablir plus efficacement. […] Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations en matière de cybersécurité. »

Mme Anne Le Hénanff, rapporteure. Je propose le retrait de l'amendement en vue d'un travail de réécriture avec l'ensemble des parties prenantes d'ici à la séance publique. À défaut, avis défavorable.

M. Éric Bothorel, rapporteur général. La rédaction de l'article est en effet problématique, notamment parce qu'elle procède à des qualifications juridiques qui n'ont pas vocation à être prévues par la loi, comme le traitement de données à caractère personnel considérées comme nécessaires à des intérêts légitimes. Sont également problématiques l'établissement d'une liste non limitative de catégories de données à caractère personnel, qui ne constitue pas une garantie, et l'absence de dispositions concernant les catégories particulières de données à caractère personnel de l'article 9 du RGPD, soit pour en exclure le traitement soit pour l'encadrer. Même avis que la rapporteure.

M. le président Philippe Latombe. Je maintiens l'amendement en espérant qu'il sera adopté et qu'une rédaction sera élaborée en vue de son examen en séance publique. Je ne voudrais pas qu'il soit oublié d'ici là.

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

Amendement CS390 de M. Philippe Latombe

M. le président Philippe Latombe. Il s'agit de s'assurer que les entités essentielles et importantes puissent être destinataires des informations concernant les menaces et qu'elles-mêmes puissent partager des informations relatives à une menace, par exemple une adresse IP, sans que l'on puisse leur opposer une autre réglementation, comme le RGPD.

Mme Anne Le Hénanff, rapporteure. Même avis que pour l'amendement précédent : avis défavorable ou demande de retrait pour la réécriture de l'amendement en vue de la séance.

M. Éric Bothorel, rapporteur général. Dans l'hypothèse d'une réécriture, je proposerai quelques éléments car, sur le fond, l'amendement prévoit des communications ou informations utiles. Toutefois, en l'état de sa rédaction, il est problématique en ce qu'il énonce que des données pourraient être « réputées respecter les législations relatives à la protection des données ». Ce respect ne peut pas être « réputé » au seul motif qu'il est envisagé par une disposition législative. Il est, en toute hypothèse, nécessaire que la communication de données personnelles soit justifiée par une finalité déterminée, explicite et légitime, et qu'elle reste proportionnée au regard de cette finalité. Même avis, donc, que Mme la rapporteure.

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

CHAPITRE III
De la supervision

Article 25 : *Prescription par l'ANSSI de mesures nécessaires en cas de cybermenaces*

Amendements identiques CS502 de M. Éric Bothorel et CS392 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il s'agit d'étendre aux agents agissant pour le compte des bureaux d'enregistrement les dispositions de l'article 25, en cohérence avec l'intégration des bureaux d'enregistrement au sein de cet article. Cette intégration se justifie par ailleurs par le besoin opérationnel de l'Anssi pour éviter un incident ou y remédier.

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

*Elle **adopte** l'article 25 **modifié**.*

Section I
Recherche et constatation des manquements

Article 26 A : (art. L. 103 du code des postes et des communications électroniques) *Services de coffre-fort numérique*

Amendements identiques CS503 de M. Éric Bothorel et CS394 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement tend à supprimer la certification par l'Anssi des services de coffre-fort numérique

*La commission **adopte** les amendements et l'article est **ainsi rédigé**.*

*En conséquence, l'amendement CS393 **tombe**.*

Article 26 : *Habilitation des agents de plusieurs organismes à rechercher et constater les manquements et infractions en matière de cybersécurité*

Amendement CS54 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Il vise à empêcher les organismes indépendants de mener des missions de contrôle. En effet, l'article 26 permet à l'Anssi de faire appel à des « organismes indépendants » dont les agents seraient habilités à de telles

missions. Or le contrôle exercé est particulièrement intrusif – il permet notamment d'accéder à des données sensibles et personnelles, et le secret professionnel n'est pas opposable. Le recours à de tels organismes pose donc des problèmes d'indépendance et d'ingérence, et complique l'action publique, ce qui est quasiment un non-sens pour le « gouvernement de la simplification ». En effet, l'Anssi doit régulièrement contrôler les organismes indépendants et les données auxquelles ils ont accès. Le recours aux prestataires privés ne peut être une solution viable lorsque des enjeux d'indépendance et de souveraineté sont concernés. Au lieu de multiplier les organismes indépendants, nous proposons de simplifier l'action publique en donnant davantage de moyens à l'Anssi, afin qu'elle puisse remplir l'ensemble de ses missions et effectuer l'ensemble des contrôles.

Mme Anne Le Hénanff, rapporteure. Il ne me semble ni opportun ni réaliste de faire peser une telle charge de travail sur l'Anssi, qui sait par ailleurs faire preuve de discernement quant au choix des prestataires et organismes indépendants. Je fais le choix de la confiance, qui est en outre le choix le plus rationnel. Avis défavorable.

M. Éric Bothorel, rapporteur général. Il faut mesurer les risques réels que comporte l'alinéa 7, qui me paraissent à la mesure du risque d'indépendance et d'ingérence évoqué par notre collègue. En effet, comme l'a précisé le directeur général de l'Anssi lors de son audition, cette agence privilégiera le recours à des prestataires qualifiés qui apportent des garanties d'indépendance. Dans les faits, les personnes concernées présenteront donc toutes les garanties nécessaires.

Le pouvoir de contrôle reste par ailleurs à l'autorité nationale, ces acteurs prêtant leur concours à ces contrôles. La constatation des manquements appartiendra aux seuls agents de l'Anssi.

L'amendement soulève, enfin, un enjeu d'opérationnalité : interdire à l'autorité nationale de s'appuyer sur ces organismes limiterait fortement sa capacité à contrôler, compte tenu de ses effectifs.

Même avis, donc, que Mme la rapporteure.

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

Amendements identiques CS505 de M. Éric Bothorel et CS395 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. La certification des services de coffre-fort numérique ayant été abrogée par l'article 26 A du projet de loi, cet amendement de cohérence vise à supprimer corrélativement la compétence de l'Anssi à contrôler le respect de cette certification.

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

Amendements identiques CS504 de M. Éric Bothorel et CS396 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement de cohérence vise à permettre de soumettre au contrôle de l'Anssi les OIV qui ne sont pas déjà soumis à son contrôle en tant qu'entité essentielle ou importante. En effet, la rédaction actuelle de l'article 26 ne couvre que les OIV des secteurs prévus par la directive NIS 2 et la directive sur la résilience des entités critiques, dite REC, alors que les OIV hors du champ des directives relèvent uniquement de l'article L. 1332-11 du code de la défense, portant les obligations qui leur sont applicables.

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

Amendements identiques CS506 de M. Éric Bothorel et CS397 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il a pour objectif d'appliquer le règlement sur la cyber-résilience (CRA) visant à imposer des exigences de cybersécurité aux fournisseurs de produits numériques accessibles sur le marché unique, qui entrera prochainement en vigueur en droit national.

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

*Elle **adopte** l'amendement rédactionnel CS398 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS399 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à compléter l'article 26 par l'alinéa suivant : « Un décret en Conseil d'État fixe les critères de délégation des audits par l'autorité nationale de sécurité des systèmes d'information à un organisme indépendant qu'elle aura désigné et les circonstances susceptibles d'exonérer l'entité contrôlée du coût du contrôle. » Afin de rendre plus lisible l'action de l'Anssi et de limiter les litiges, il importe de clarifier les conditions de choix des opérateurs des contrôles, ainsi que les raisons qui pourraient permettre d'exonérer les entités contrôlées du coût du contrôle.

Mme Anne Le Hénanff, rapporteure. Il me semble satisfait par l'alinéa 7 de l'article 26, qui prévoit déjà une habilitation des agents et personnels des organismes indépendants ou experts.

M. Éric Bothorel, rapporteur général. Il est même doublement satisfait parce que l'article 30 prévoit que les modalités d'application sont précisées par décret en Conseil d'État. En outre, l'autorité nationale reste responsable du contrôle et n'en déléguera pas la responsabilité, l'organisme indépendant lui prêtant, le cas échéant, son concours dans cette mission. Même avis que Mme la rapporteure.

*L'amendement est **retiré**.*

*La commission **adopte** l'article 26 **modifié**.*

Article 27 : *Droits et obligations des agents chargés d'un contrôle de l'ANSSI et de la personne contrôlée*

Amendements identiques CS27 de M. Denis Masséglia et CS30 de Mme Sabine Thillaye

M. Denis Masséglia (EPR). L'article 27 du projet de loi confère aux agents de l'Anssi la faculté, lors de contrôles, d'accéder aux systèmes d'information et aux données d'une entité, sans que celle-ci puisse invoquer le secret des affaires. Une telle prérogative touche pourtant des éléments sensibles, essentiels à la compétitivité et à la stratégie des entreprises. Il apparaît donc indispensable d'encadrer davantage ce droit d'accès afin de préserver la confidentialité des informations commerciales les plus critiques. L'amendement vise ainsi à introduire un critère de nécessité pour mieux apprécier et objectiver la légalité des demandes d'accès et offrir un niveau renforcé de sécurité juridique.

Mme Anne Le Hénanff, rapporteure. Ces amendements me semblent satisfaits. Je ne partage pas l'idée qu'il y ait un risque de ce point de vue et qu'il soit donc nécessaire d'encadrer davantage le droit d'accès, notamment des agents de l'Anssi, aux données. Avis défavorable.

M. Éric Bothorel, rapporteur général. L'introduction d'un critère de nécessité permet d'apporter des garanties entourant les mesures de supervision et d'exécution. Avis très favorable.

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

Amendement CS400 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il tend à supprimer de l'alinéa 6 la mention « qui doit comporter les questions auxquelles il est répondu ». En effet, imposer lors d'un contrôle la rédaction des questions auxquelles les entités doivent répondre correspond, dans les faits, à une exigence prévue dans le cadre des procédures pénales et non en contrôle de nature administrative. Cette exigence est, en outre, source de complexité, voire irréaliste, tant pour les contrôleurs que pour l'entité contrôlée compte tenu du déroulement pratique d'un contrôle en matière de systèmes d'information, où les demandes et échanges se succèdent. L'entité peut par ailleurs, en tout état de cause, faire des observations dans le procès-verbal. La lecture du procès-verbal est aussi prévue en procédure pénale et introduit une exigence inutile dans la loi.

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

Amendement CS507 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Il tend à compléter les prérogatives des agents et personnels chargés des contrôles des entités assujetties en ouvrant la possibilité de prélever des échantillons de produits.

Mme Anne Le Hénanff, rapporteure. Sagesse.

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

Amendement CS52 de M. René Pilato

Mme Anne Le Hénanff, rapporteure. Cet amendement me semble déjà satisfait. Par ailleurs, la mention : « sans délai à partir du moment où il est constaté qu'ils ne sont plus nécessaires à l'instruction » me semble très contraignante. Avis défavorable.

M. Éric Bothorel, rapporteur général. S'agissant de la suppression de tout document collecté à l'issue de l'instruction, cette proposition n'est pas compatible avec l'ensemble de la procédure de supervision. En effet, la conservation des éléments de preuve de nature à établir les manquements est nécessaire non seulement pour mener la procédure de supervision à son terme devant la commission des sanctions, mais également en cas de contentieux contestant les mesures d'exécution que l'Anssi est susceptible de prendre lors de l'instruction. Avis défavorable.

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

Amendement CS53 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Il vise à inscrire dans la loi qu'aucun document qui relève du secret professionnel ne pourra être copié ou retranscrit par les agents, qui seront ainsi limités à leur seule consultation, nécessaire pour permettre un contrôle effectif de la cybersécurité d'un organisme.

Mme Anne Le Hénanff, rapporteure. La loi encadrant déjà ces situations, l'amendement est satisfait. Avis défavorable.

M. Éric Bothorel, rapporteur général. La plupart des documents détenus par les entités et pouvant être demandés lors d'un contrôle sont susceptibles, en tout ou partie, de contenir des informations relevant du secret professionnel. La restriction proposée risque d'entraver, voire d'empêcher, le déroulement du contrôle et de l'instruction, qui visent justement à évaluer, notamment sur pièces, l'existence ou non de manquements. En outre, certains contrôles ont lieu sur pièces, et non sur place. Enfin, les agents et personnels chargés du contrôle sont eux-mêmes soumis au secret professionnel pour les faits, actes ou renseignements dont ils ont connaissance en raison de leurs fonctions, ce qui offre la garantie de préservation du secret professionnel entrant dans le périmètre du contrôle. Avis défavorable.

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

*Elle **adopte** l'article 27 **modifié**.*

La séance est levée à minuit.

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Réunion du mardi 9 septembre 2025 à 21 h 30

Présents. - M. Éric Bothorel, M. Mickaël Bouloux, Mme Marina Ferrari, Mme Olga Givernet, Mme Catherine Hervieu, M. Philippe Latombe, Mme Anne Le Hénanff, M. Aurélien Lopez-Liguori, M. Denis Masséglia, M. Paul Midy, M. Jacques Oberti, Mme Marie Récalde, Mme Véronique Riotton, M. Arnaud Saint-Martin, M. Emeric Salmon, M. Hervé Saulignac, Mme Sabrina Sebaihi, Mme Liliana Tanguy, M. Vincent Thiébaut, Mme Sabine Thillaye, M. Antoine Villedieu