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

Mercredi 10 septembre 2025

Séance de 14 heures

Compte rendu n° 19

SESSION EXTRAORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à quatorze heures.

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).

Article 28 : *Devoir de coopération de la personne contrôlée et amende administrative en cas d'obstacle à un contrôle*

Amendements CS156 de Mme Marina Ferrari et CS229 de M. Aurélien Lopez-Liguori (discussion commune)

Mme Marina Ferrari (Dem). Élaboré avec le Medef, mon amendement vise à rendre la sanction plus proportionnée.

M. Aurélien Lopez-Liguori (RN). L'article 28 prévoit que l'Agence nationale de la sécurité des systèmes d'information (Anssi) inflige une amende administrative aux entités qui ne coopéreraient pas ou qui fourniraient des informations inexactes ou incomplètes. Cependant, dans sa rédaction actuelle, il ne fait pas de distinction entre une obstruction volontaire et une erreur de bonne foi, alors même que celle-ci serait plausible de la part des nouveaux assujettis à la directive NIS 2 (Network and Information Security) – les démarches administratives sont parfois très complexes, en particulier pour les petites entités. Ainsi, les petites collectivités locales qui commettraient des omissions involontaires par méconnaissance risquent la même sanction qu'un acteur qui aurait délibérément cherché à tromper les autorités. Cela va à l'encontre du principe fondamental de proportionnalité des sanctions figurant dans le droit français, mais aussi de l'article 34 de la directive NIS 2, exigeant des mesures effectives, proportionnées et dissuasives.

Cet amendement introduit une clarification simple : la sanction ne doit s'appliquer qu'en cas de manquement volontaire.

Mme Anne Le Hénanff, rapporteure. Avis favorable à l'amendement CS156, qui apporte une précision opportune en reconnaissant le droit à l'erreur, auquel je suis attachée. Je suis en revanche défavorable à l'amendement CS229, qui me semble moins bien rédigé.

M. Éric Bothorel, rapporteur général. La commission des sanctions prévue dans le présent projet de loi tient déjà compte du caractère intentionnel des fautes, prise en considération qui a été renforcée par un amendement sénatorial. Pour les deux amendements, demande de retrait ou avis défavorable.

*La commission **rejette** successivement les amendements CS156 et CS229.*

Amendements identiques CS16 de M. Denis Masséglia et CS154 de Mme Marina Ferrari

M. Denis Masséglia (EPR). L'article 28 prévoit que l'entité contrôlée coopère avec l'Anssi, tout manquement étant passible d'une amende administrative. Toutefois, en matière de sanctions, le texte n'établit pas de distinction entre entités essentielles et entités importantes, contrairement à la directive NIS 2.

Cet amendement vise à préciser les différentes sanctions en fonction des catégories d'entités, afin que la transposition soit aussi fidèle que possible à la directive NIS 2. C'est en effet en homogénéisant les transpositions de directives que nous pourrons accompagner nos entreprises dans leur développement dans tous les pays de l'Union européenne.

Mme Anne Le Hénanff, rapporteure. Ces amendements s'inscrivent dans la logique de la directive NIS 2 et sont mieux rédigés que l'alinéa. Avis favorable.

M. Éric Bothorel, rapporteur général. Je m'en remets à la sagesse des membres de la commission.

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

*En conséquence, l'amendement CS402 de Mme Le Hénanff, rapporteure, **tombe**.*

*La commission **adopte** l'amendement rédactionnel CS403 de Mme Le Hénanff, rapporteure.*

Amendement CS172 de Mme Sabrina Sebaihi

Mme Sabrina Sebaihi (EcoS). Il vise à ne pas imposer de sanctions financières aux collectivités locales. C'est à elles plutôt qu'aux grandes entreprises que le texte demande un effort financier, alors même que leurs budgets ont connu d'importantes coupes ces dernières années. Il faut au contraire les accompagner dans leurs investissements en matière de cybersécurité.

Dans une logique de responsabilité et de justice, nous proposons de remplacer les sanctions financières par des outils plus efficaces, comme la publicité des injonctions, l'accompagnement et la formation. Il s'agit de mettre les élus face à leurs responsabilités, sans pénaliser ni fragiliser les services publics.

Mme Anne Le Hénanff, rapporteure. L'équilibre trouvé au Sénat s'agissant des collectivités me semble bon. Avis défavorable.

M. Éric Bothorel, rapporteur général. Ce débat est légitime, notamment à la lumière de l'éclairage apporté par le Conseil d'État au point 9 de son avis. Nous l'aurons à nouveau en séance publique à propos d'un amendement de M. le président.

Avis défavorable également.

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

*Elle **adopte** l'article 28 **modifié**.*

Article 29 : *Forme et prise en charge financière des contrôles*

*La commission **adopte** successivement les amendements rédactionnels CS404 et CS405 de Mme Le Hénanff, rapporteure.*

Amendements CS34 de Mme Sabine Thillaye et CS230 de M. Aurélien Lopez-Liguori (discussion commune)

Mme Sabine Thillaye (Dem). L'article 29 prévoit que l'Anssi peut déléguer l'exécution des contrôles à des organismes indépendants. Compte tenu du caractère très sensible des données récoltées à cette occasion, mon amendement vise à préciser que le siège social de ces organismes doit se situer dans un État membre de l'Union européenne.

M. Aurélien Lopez-Liguori (RN). Mon amendement est un peu plus précis, puisqu'il porte non pas sur le siège social, mais sur le siège statutaire, l'administration centrale et l'établissement principal d'une entreprise qui procéderait aux audits.

Que l'Anssi puisse déléguer des contrôles à des organismes indépendants est une bonne chose. Toutefois, contrôler la cybersécurité d'une entité importante ou essentielle n'est pas un acte banal : cela donne accès à des points sensibles de nos infrastructures vitales ; cela conduit à manipuler des informations classifiées ; cela met au jour des vulnérabilités que nos adversaires rêveraient de connaître.

Nous ne pouvons accepter que de tels contrôles soient confiés à des acteurs étrangers, potentiellement soumis à des législations extraterritoriales ou à des intérêts extérieurs ; nous serions inconscients de le laisser faire. La cybersécurité doit rester dans le domaine régalien et ne pas être déléguée à des puissances étrangères, en particulier s'agissant d'opérateurs d'importance vitale (OIV) : il s'agit d'une ligne rouge. Les contrôles ne doivent être effectués que par des organismes à tout le moins européens, uniquement soumis au droit européen.

Mme Anne Le Hénanff, rapporteure. Nous avons déjà eu ce débat hier soir et je n'ai pas changé d'avis : ces amendements visent à surtransposer la directive NIS 2.

Il importe que les organismes indépendants soient certifiés par l'Anssi, qu'on ne peut soupçonner de vouloir mettre en danger la sécurité nationale et la souveraineté. Avis défavorable.

M. Éric Bothorel, rapporteur général. Je partage cet avis. Une préférence européenne ou, en tout cas, un privilège européen est souhaitable, mais le présent texte n'a pas vocation à créer une norme, qui serait source d'insécurité pour les entreprises. Une telle initiative doit être lancée au niveau européen.

M. Aurélien Lopez-Liguori (RN). L'Anssi est une autorité administrative, qui applique le droit français ; elle ne dispose pas de moyens de protéger le pays contre l'extraterritorialité, sauf si nous les lui fournissons.

Quant à la sécurité de nos entreprises, elle n'est pas menacée puisque l'audit est diligenté par l'Anssi. Mais parce que celle-ci sera contrainte, pour différentes raisons, de recourir à des cabinets d'audit, nous souhaitons empêcher que ces derniers soient extra-européens. Une telle mesure contribuera à créer des emplois européens tout en protégeant nos entreprises.

La surtransposition est critiquable uniquement lorsqu'elle pose des problèmes de concurrence ou de simplification.

Mme Anne Le Hénanff, rapporteure. Je souscris à votre analyse, mais le véhicule législatif n'est pas le bon. Nous devrons très probablement travailler sur cet enjeu, mais pas dans le cadre de cette transposition.

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

Amendement CS231 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Il s'agit d'un amendement de repli, visant à donner aux entreprises elles-mêmes les moyens de se prémunir contre l'intervention de cabinets d'audit extra-européens : elles auraient la possibilité d'utiliser une sorte de droit de veto pour refuser qu'une entreprise américaine ou canadienne contrôle leurs systèmes d'information.

Mme Anne Le Hénanff, rapporteure. Avis défavorable, pour les mêmes raisons que celles exposées précédemment.

M. Éric Bothorel, rapporteur général. L'Anssi est une autorité administrative, certes, mais c'est bien une autorité : elle désignera les organismes habilités à effectuer des audits de sécurité sur la base d'une liste d'entités de confiance avec lesquelles elle travaille depuis plusieurs années. On peut se fier à elle pour les audits d'entités particulièrement sensibles, comme les OIV ; elle sera en mesure de prévenir tout risque de compromission ou d'ingérence étrangère, sans qu'il soit nécessaire de l'inscrire dans ce texte.

Dès que des informations classifiées sont concernées, les règles de l'instruction générale interministérielle (IGI) n° 1300 sur la protection du secret de la défense nationale (PSDN) s'appliquent. Ces garanties sont suffisantes pour protéger les informations confidentielles auxquelles les organismes chargés des audits pourraient accéder. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). J'entends votre position consistant à dire que l'Anssi a toutes les compétences pour nous défendre de l'extraterritorialité et des ingérences, mais elle n'a pas nécessairement les outils suffisants.

Allons plus loin : l'Anssi a-t-elle empêché l'État français de solliciter Microsoft pour développer le Health Data Hub, alors que le risque d'ingérence était connu ? A-t-elle empêché l'avant-dernier gouvernement de passer un contrat de plus de 250 millions d'euros avec l'entreprise canadienne CGI pour procéder à des audits de cybersécurité et mener des formations dans les ministères ? Non.

Pourquoi l'Anssi n'a-t-elle rien fait ? Parce qu'elle ne dispose pas des outils lui permettant d'agir. Les lui octroyer relèverait certes d'une démarche de surtransposition, mais nous ne disposons pas d'un autre véhicule législatif. Nous ne savons pas quand nous aurons l'occasion de reparler de cybersécurité, alors que la situation est urgente : nous sommes confrontés à des enjeux de souveraineté, de résilience et d'indépendance. Le temps nous manque et en tant que législateur, nous devons saisir toutes les occasions ; ce texte en est une.

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

Amendement CS173 de Mme Sabrina Sebaihi

Mme Sabrina Sebaihi (EcoS). Il vise à exonérer les collectivités du financement des audits. On leur demande de faire davantage avec des moyens de plus en plus contraints, mais c'est à ceux qui rendent ces audits obligatoires de les financer.

Il serait préférable d'augmenter les dotations aux collectivités pour leur permettre de financer ces audits, plutôt que de les étrangler financièrement en les y contraignant.

Mme Anne Le Hénanff, rapporteure. Je répète que, s'agissant des collectivités territoriales, l'équilibre trouvé au Sénat est le bon ; il n'y a pas de raison de les exempter du financement des audits.

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

Amendement CS459 de Mme Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il vise à laisser les entités mentionnées à l'article 14 du texte choisir les prestataires de services certifiés, qualifiés ou agréés ou les organismes indépendants sur la base d'une liste élaborée par l'Anssi.

Cette demande a été régulièrement formulée lors des auditions, pour différentes raisons – il n'est pas toujours souhaitable qu'une société en audite une autre. Il me semble nécessaire de permettre aux entités contrôlées de choisir entre différents auditeurs, notamment pour des raisons de confidentialité.

M. Éric Bothorel, rapporteur général. Demande de retrait ou avis défavorable.

Le recours à des dispositifs matériels ou logiciels ou à des prestataires de services certifiés, qualifiés ou agréés, ainsi que la présomption de leur conformité, figurent à l'article 16 du présent texte. Les audits de sécurité réguliers réalisés par des organismes indépendants sont déjà concernés. Ces exigences spécifiques sont applicables aux OIV en ce qui concerne leurs systèmes d'information d'importance vitale et aux administrations en ce qui concerne leurs systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations, soumis au référentiel général de sécurité (RGS) des systèmes d'information.

Le dispositif de cet amendement, qui vise les entités mentionnées à l'article 14, ne semble donc pas opérant et ne correspond pas au besoin exprimé dans l'exposé des motifs du projet de loi.

En outre, l'Anssi publie déjà sur son site internet une liste de prestataires de services qualifiés. Cependant, puisque l'on peut considérer que cette publication ne satisfait pas le besoin exprimé, nous pourrons travailler à une meilleure rédaction du texte d'ici à son examen en séance publique.

Mme Anne Le Hénanff, rapporteure. J'entends votre proposition d'amélioration rédactionnelle, mais je tiens à ce que les personnes auditionnées sachent que leur avis a été pris en considération. Je maintiens mon amendement.

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

*Elle **adopte** l'article 29 **modifié**.*

Article 30 : *Modalités d'application des dispositions relatives aux prérogatives de l'Anssi en matière de recherche et de constatation des manquements*

Amendement CS406 de M. Philippe Latombe

M. Philippe Latombe, président. Il s'agit d'un amendement d'appel.

Depuis les déclarations de la ministre chargée du numérique et du directeur général de l'Anssi lors de leurs auditions par les commissions spéciales du Sénat ou de l'Assemblée, le délai de trois ans semble faire consensus, mais aucune trace écrite n'en existe à ce jour. Le projet de loi ne prévoit pas de date limite pour la mise en conformité, ni pour l'application des contrôles et des sanctions potentielles.

L'Anssi a indiqué qu'elle laisserait aux entités le temps de se mettre en conformité avant d'engager les procédures de contrôle et d'appliquer les sanctions. Afin d'assurer une lisibilité et de permettre une certaine progressivité de la mise en conformité tout en encourageant les entités à ne pas attendre le dernier moment pour remplir leurs obligations, il est nécessaire de fixer un calendrier d'application échelonnée et différenciée des mesures de contrôle, tenant compte du niveau de préparation des entités concernées et du niveau de priorité des exigences de mise en conformité.

Cet amendement fait écho à une discussion que nous avons eue hier : des engagements qui avaient été pris au banc par le ministre lors de l'examen de la loi de programmation militaire (LPM) ont été modifiés *a posteriori*. Il est donc nécessaire que le législateur fasse figurer dans le projet de loi ce qui a été dit lors des auditions et qui constitue la base de notre accord.

Mme Anne Le Hénanff, rapporteure. L'établissement d'un calendrier me semble trop contraignant : il ne me semble pas opportun de figer une procédure dans la loi. L'Anssi et les entités concernées sont capables de travailler en bonne intelligence. Avis défavorable.

M. Philippe Latombe, président. Je maintiens cet amendement. S'il n'est pas adopté, je le déposerai pour l'examen du texte en séance publique, afin que nous ayons un engagement ferme du futur ministre du numérique.

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

Amendement CS232 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Il vise à simplifier l'écosystème cyber. La Cnil (Commission nationale de l'informatique et des libertés) et l'Anssi disposent toutes deux de compétences de contrôle pouvant porter sur les mêmes entités, susceptibles de conduire à des doublons de procédure et à une charge administrative excessive ; leurs appréciations peuvent être différentes, voire contradictoires : la situation est non seulement inefficace, mais peut être dangereuse. À l'heure où les cyberattaques exigent une réponse rapide et coordonnée, nous ne pouvons pas nous permettre de tels chevauchements bureaucratiques. Nous proposons de prévoir une coordination explicite entre la Cnil et l'Anssi, notamment pour organiser des contrôles conjoints, alternés ou séquencés, dans le respect des compétences propres de chaque autorité. La cybersécurité exige de l'unité, pas de la dispersion. Nos autorités doivent avoir les moyens d'agir ensemble et efficacement, au service de la sécurité nationale.

Mme Anne Le Hénanff, rapporteure. La précision relative aux modalités de coordination avec la Cnil ne me semble pas indispensable. Le directeur de l'Anssi a précisé, lors de son audition, qu'en cas d'absence de respect du RGPD (règlement général sur la protection des données) clairement constatée lors d'un audit ou d'un contrôle, l'Anssi saisirait la Cnil. Avis défavorable.

M. Éric Bothorel, rapporteur général. Si tel n'est pas toujours le cas, il est un point sur lequel je suis d'accord avec M. de Courson : l'usage du mot « notamment » dans le droit n'est pas utile. Avis défavorable.

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

Elle ***adopte*** *l'article 30* ***non modifié****.*

Section 2
Mesures consécutives aux contrôles

Article 31 : *Ouverture d'une procédure à l'encontre de la personne contrôlée*

Amendements identiques CS508 de M. Éric Bothorel et CS407 de Mme Anne Le Hénanff, amendement CS155 de Mme Marina Ferrari (discussion commune)

Mme Anne Le Hénanff, rapporteure. Mon amendement est un amendement de clarification. L'alinéa 1er de l'article 31 doit prévoir des conditions de déclenchement de la phase d'instruction compatibles avec la réalité opérationnelle des contrôles. Si tel est effectivement le cas lorsque, de manière évidente, les mesures de contrôle ont révélé un manquement, cela doit également être possible lorsque le constat de certains faits est susceptible de révéler un manquement qui n'est pas encore qualifié ou pleinement établi au moment de l'ouverture de l'instruction. Dans certaines hypothèses, la qualification d'un manquement nécessitera des mesures d'instruction approfondies, assorties, le cas échéant, de mesures de contrôle complémentaires. La phase d'instruction permettra ainsi la qualification de certains faits compte tenu des réglementations mentionnées à l'article 26, pour déterminer si des manquements peuvent être identifiés. Il ne faut donc pas limiter l'ouverture de la phase d'instruction aux manquements constatés et qualifiés dans le cadre des mesures de contrôle.

Mme Marina Ferrari (Dem). L'amendement CS155 vise à supprimer les mots « ou une suspicion de manquement », qui ne figurent pas dans la directive NIS 2 et afin de garantir le droit à l'erreur.

Mme Anne Le Hénanff, rapporteure. J'ai échangé avec l'Anssi sur ce point : il est indispensable de conserver les mots « ou une suspicion de manquement », car il est souvent difficile d'établir avec certitude l'existence d'un manquement. En leur absence, de très nombreux cas où la suspicion est caractérisée ne seraient pas soumis à l'Anssi, au seul motif qu'elle n'a pas été en mesure de la caractériser de manière formelle. Avis défavorable.

L'amendement CS155 est ***retiré****.*

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

Amendement CS408 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement de clarification vise à préciser que les astreintes seront prononcées par l'autorité nationale de sécurité des systèmes d'information.

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

*Elle **adopte** l'article 31 **modifié**.*

Article 32 : *Mesures d'exécution*

*La commission **maintient la suppression de** l'article 32.*

Article 33 : *Saisine par l'Anssi de la commission des sanctions*

Amendement CS233 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). L'article 33 permet la saisine de la commission des sanctions sans préciser que la personne contrôlée en est informée. Or, dans toute procédure administrative et disciplinaire, cette information constitue une garantie élémentaire qui permet à la personne visée de mieux préparer sa défense, d'apporter ses observations et de collaborer de manière constructive. Sans cette précision, nous risquons d'introduire une insécurité juridique : les sanctions seront susceptibles d'être contestées sur la forme faute de respect du principe du contradictoire.

Le présent amendement vise à inscrire noir sur blanc le caractère obligatoire de l'information préalable. L'objectif n'est pas d'alourdir la procédure mais de la rendre plus robuste, transparente et légitime.

Mme Anne Le Hénanff, rapporteure. Cet ajout me semble pertinent. Avis favorable.

M. Éric Bothorel, rapporteur général. La saisine de la commission des sanctions faisant toujours suite à la notification des griefs, l'article 33 n'a pas besoin de prévoir explicitement l'information de la personne concernée par la procédure de sanction : cet amendement est satisfait. Avis défavorable.

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

Amendements identiques CS509 de M. Éric Bothorel et CS410 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. L'amendement CS410 apporte des modifications de coordination. Il tend, à titre principal, à tirer les conséquences de précédents amendements qui excluent du champ de la directive NIS 2 les personnes morales dont les activités sont visées à l'article L. 1332-2 du code de la défense, tout en garantissant qu'elles font l'objet d'un niveau d'exigence équivalent. Il permet ainsi de soumettre ces personnes aux mesures consécutives à un contrôle prévues à l'article 33.

Il vise également à remplacer la notion d'entité par celle de personne concernée, dans la mesure où les personnes morales précitées, n'ayant pas la qualité d'entité essentielle ou importante, ne sauraient donc être considérées comme des entités au sens de la directive.

Enfin, cet amendement vise à simplifier la rédaction de l'alinéa 3 de l'article 33 en supprimant la mention des articles 8 et 10.

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

*Elle **adopte** l'amendement rédactionnel CS409 de Mme Anne Le Hénanff, rapporteure.*

*La commission **adopte** l'article 33 **modifié**.*

Après l'article 33

Amendements identiques CS510 de M. Éric Bothorel et CS185 de M. Vincent Thiébaut

M. Vincent Thiébaut (HOR). L'amendement CS185 vise à sécuriser juridiquement la dématérialisation des actes établis par les agents et personnels compétents. Cette mesure de bon sens prévoit l'utilisation d'une signature électronique unique et sécurisée, conforme aux standards techniques : elle assurera la valeur probante des actes, quels que soient le nombre de pages ou de signataires. L'objectif est de moderniser et simplifier les procédures administratives, conformément à l'exigence de sobriété normative.

*Suivant l'avis de la rapporteure, la commission **adopte** les amendements.*

Article 34 : *Modalités d'application des dispositions relatives à la procédure pouvant être engagée par l'Anssi à l'encontre de la personne contrôlée*

*La commission **adopte** l'amendement rédactionnel CS411 de Mme Anne Le Hénanff, rapporteure.*

*La commission **adopte** l'article 34 **modifié**.*

Section 3
Des sanctions

Article 35 : *Compétence de la commission des sanctions*

*La commission **adopte** l'article 35 **non modifié**.*

Article 36 : *Composition de la commission des sanctions*

Amendement CS412 de M. Philippe Latombe

M. le président Philippe Latombe. L'objectif est de s'assurer que la sanction éventuelle prend en compte, d'une part, l'impact des manquements de l'entité visée à ses obligations sur ses clients, ses fournisseurs ou son écosystème et, d'autre part, les enjeux stratégiques – notamment l'intelligence économique –, économiques, technologiques ou sociaux liés à l'entité. L'expertise sectorielle d'un représentant du ministère en charge du secteur d'activité de l'entité visée complétera les expertises techniques et juridiques des autres membres de la commission des sanctions.

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

Amendements identiques CS511 de M. Éric Bothorel, CS415 de Mme Anne Le Hénanff et CS157 de Mme Marina Ferrari

Mme Anne Le Hénanff, rapporteure. Il s'agit d'aligner, par cohérence, les conditions et garanties quant à la nomination des personnalités qualifiées sur celles prévues pour la composition de la commission des sanctions mentionnée au titre I^{er}.

Il s'agit également de ne pas limiter la possibilité de recourir à des personnes dont la compétence en matière cyber est avérée afin d'éclairer la décision de la commission des sanctions. Un mécanisme de déport permettrait, lorsque le dossier l'impose, de prévenir le risque de conflit d'intérêts, à l'instar de ce qui existe dans d'autres instances prononçant des sanctions. Il serait donc disproportionné de prévoir des incompatibilités conduisant à se priver de potentiels candidats au profil intéressant.

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

En conséquence, l'amendement CS158 de Mme Marina Ferrari et les amendements CS413 et CS414 de Mme Anne Le Hénanff, rapporteure, ***tombent****.*

L'amendement CS159 de Mme Marina Ferrari est ***retiré****.*

La commission ***adopte*** *l'article 36* ***modifié****.*

Article 37 : *Sanctions en cas de manquements aux obligations en matière de cybersécurité*

La commission ***adopte*** *l'amendement rédactionnel CS416 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS515 de M. Éric Bothorel et CS418 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Mon amendement a pour objet de tirer les conséquences de précédents amendements qui soumettent aux obligations des articles 14 et 17 les personnes morales que leurs activités visées à l'article L. 1332-2 du code de la défense privent de la qualité d'entité essentielle ou importante : il les soumet également au dispositif de sanction prévu à l'article 37.

Il vise par ailleurs à remplacer la notion d'entité importante ou essentielle par la celle de personne concernée, dans la mesure où les personnes morales visées, n'ayant pas la qualité d'entité essentielle ou importante, ne sauraient dès lors être considérées comme des entités au sens de la directive.

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

Amendements CS234 de M. Aurélien Lopez-Liguori et CS28 de Mme Sabine Thillaye (discussion commune)

M. Aurélien Lopez-Liguori (RN). C'est une question de justice : l'amendement CS234 vise à remédier à l'asymétrie selon laquelle le secteur public – dont les collectivités territoriales, leurs groupements et leurs établissements publics administratifs – serait exclu du régime de sanctions administratives applicable aux autres secteurs. Un opérateur privé dans le domaine de la gestion de l'eau ou des déchets serait susceptible d'être sanctionné d'une amende en cas de manquement à la directive NIS 2, tandis qu'une régie municipale exploitant les mêmes services essentiels y échapperait totalement. Ainsi, France Travail ne serait pas sanctionnée en cas de perte de données similaire à celle qui a eu lieu il y a quelques mois.

Or une cyberattaque ne fait pas de distinction selon qu'un service d'eau potable est fourni par une entreprise privée ou par une collectivité : les risques pour les Français sont identiques. Le Conseil d'État a lui-même relevé cette incohérence, en rappelant que la directive européenne NIS 2 prévoit des sanctions « effectives, proportionnées et dissuasives » pour toutes les entités concernées, publiques ou privées. Exonérer les collectivités de sanctions exposerait la France à un double risque, juridique – au niveau européen, alors que vous ne cessez d'affirmer depuis le début de l'examen du texte qu'il s'agit de nous soumettre à nos obligations à cet égard – et opérationnel, en affaiblissant l'efficacité de l'ensemble du dispositif de résilience. En l'absence de sanction ou d'un mécanisme d'effet équivalent, comment garantir que les collectivités se mettront en conformité avec leurs obligations ? Comment s'assurer que les services essentiels qu'elles gèrent sont protégés avec le même sérieux que ceux relevant d'acteurs privés ?

Mme Sabine Thillaye (Dem). Dans le cadre de l'application de la directive NIS 2, le projet de loi soustrait au régime des sanctions administratives les administrations de l'État et ses établissements publics administratifs, ainsi que les collectivités territoriales. Le Conseil d'État estime qu'une telle différence de traitement avec les opérateurs privés n'est pas justifiée, même si le gouvernement dispose à leur égard d'autres moyens que ces amendes pour garantir le respect de leurs obligations. Il ne faut pas laisser de faille dans le système.

Mme Anne Le Hénanff, rapporteure. Avis défavorable. On ne peut pas mettre sur le même plan une entreprise privée, à but lucratif – pour son dirigeant, la pire des sanctions est financière – et les collectivités, qui œuvrent pour l'intérêt général et le service public – même si elles créent des entités à statut spécifique dont il faudra peut-être que nous nous demandions, avec l'Anssi, comment les sanctionner à l'avenir.

Je travaille depuis dix ans sur la cybersécurité dans les collectivités locales. Dans un contexte politique où les maires sont submergés d'obligations, de contraintes, de réglementations et de contrôles, où leurs qualités et leurs compétences sont mises en doute, une sanction financière serait extrêmement mal vécue. Pour un maire, la pire des sanctions n'est pas financière – intégrée au budget, elle passe presque inaperçue –, mais une mauvaise réputation liée à la publication de son manquement à ses obligations en matière de protection des données, créant un risque pour l'élection suivante. Une sanction financière serait inutile et créerait des tensions avec les collectivités territoriales.

M. Éric Bothorel, rapporteur général. Avis défavorable, pour des raisons différentes. Les attaquants ne se feront pas de nœuds au cerveau pour distinguer ceux qui ont du pognon de ceux qui exercent une mission de service public – il suffit pour s'en convaincre de voir les conditions d'utilisation du rançongiciel Lockbit. L'utilité sanitaire d'un hôpital ou la mission de service public d'une collectivité ne dissuadera pas de les attaquer ! Conformons-nous aux observations formulées par le Conseil d'État au point 9 de son avis sur le projet de loi. Je vous invite à retirer vos amendements au profit de celui qui sera défendu plus tard par le président : il introduira une graduation, évitant ainsi un pur parallélisme des formes entre les entreprises privées et le secteur public.

Mme Sabine Thillaye (Dem). La commission des sanctions procède à une évaluation et n'est pas obligée d'appliquer une sanction. Si je comprends vos arguments, madame la rapporteure, le sujet n'est pas suffisamment pris au sérieux par les collectivités. Il est nécessaire de pouvoir disposer d'au moins un instrument.

M. Aurélien Lopez-Liguori (RN). Il s'agit d'un amendement d'appel. La sanction financière n'est pas forcément la bonne solution, *a fortiori* pour les collectivités territoriales. Réfléchissons, d'ici la séance, à votre idée, monsieur le rapporteur général, par exemple une obligation de communication dans la presse locale. Si les collectivités sont les plus nombreuses à être concernées, il ne faut pas oublier les agences de l'État – ou les ministères –, pour lesquelles il faudra trouver une solution : elles ne procèdent pas de l'élection et se fichent de la communication comme de l'amende, qui ne sera pas payée avec leur argent.

Mme Sabrina Sebaihi (EcoS). Le département des Hauts-de-Seine a subi une cyberattaque le 19 mai dernier et des dizaines de dossiers de la MDPH (maison départementale des personnes handicapées) ont disparu des serveurs ; cela signifie que les familles n'ont plus de notification, qu'il faut tout reprendre de zéro. Au-delà du coût financier – qui peut être absorbé, comme vous l'avez dit, madame la rapporteure –, il faut aussi tenir compte du coût humain et social d'une telle situation.

L'essentiel est donc d'accompagner les collectivités en matière de sécurité pour éviter qu'elles subissent ce genre d'attaques, au lieu de vouloir les sanctionner alors qu'elles sont déjà très sensibilisées et décidées à protéger les données de leurs usagers – elles prennent très au sérieux les enjeux de sécurité.

Nous voterons donc contre les amendements.

Mme Marina Ferrari (Dem). Il se trouve que, dans mes anciennes fonctions au gouvernement, j'ai été à l'origine de l'exonération de la sphère publique du dispositif de sanctions. J'ai fait cet arbitrage pour plusieurs raisons. D'abord, et cela a été exprimé dans l'avis du Conseil d'État, il semblait compliqué d'estimer l'assiette sur laquelle porterait l'amende, puisqu'il est difficile d'évaluer le chiffre d'affaires d'une collectivité – si certaines disposent d'une régie lorsqu'elles sont opératrices de l'eau notamment, ce n'est pas le cas de toutes.

Ensuite, j'entends l'argument concernant les agences de l'État, mais on ne parle là que d'opérations comptables : on donne de l'argent d'un côté et on le reprend de l'autre par le biais d'une d'amende – c'est un peu baroque ! C'est comme les indemnisations accordées aux agriculteurs : on les aide d'un côté et on fiscalise de l'autre.

Enfin, je rappelle que si la directive NIS 2 permet aux États membres de soumettre les collectivités aux sanctions, la décision relève d'un choix politique. À l'époque, le choix du gouvernement avait été de ne pas assujettir les collectivités aux sanctions.

En revanche, je comprends la nécessité de trouver un aiguillon pour inciter les collectivités à s'engager et à aller plus vite ; la menace réputationnelle en est un – même si j'admets qu'elle affectera moins les agences de l'État.

Nous verrons si la rédaction proposée dans l'amendement du président nous convient, mais il faudra sans doute y retravailler d'ici à la séance.

La réunion est brièvement suspendue.

Les amendements CS234 et CS28 sont ***retirés****.*

Amendements identiques CS516 de M. Éric Bothorel et CS417 de M. Philippe Latombe

M. le président Philippe Latombe. Nous faisons tous le même constat : si le Conseil d'État a considéré que nous ne pouvions pas exonérer de sanctions financières la totalité des collectivités territoriales et des agences de l'État, il n'en reste pas moins qu'il sera difficile, comme l'a souligné Mme Ferrari, d'en déterminer l'assiette.

C'est pourquoi je propose de supprimer aux alinéas 2 et 3 de l'article les mots « collectivités territoriales », « groupements » et « établissements publics administratifs » et d'insérer un nouvel alinéa ainsi rédigé : « En cas de manquement aux obligations prévues au présent titre, la commission des sanctions enjoint aux collectivités territoriales de mettre en place un plan de remédiation dans un délai d'une semaine » – nous pourrons bien sûr discuter de ce délai – « à compter de la constatation du manquement. Si le plan de remédiation n'a pas été mis en place, la commission des sanctions peut prononcer à l'encontre de la collectivité territoriale une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ».

Cet amendement permet de répondre aux remarques du Conseil d'État s'agissant de la constitutionnalité du dispositif et d'établir une graduation, en prévoyant dans un premier temps un plan de remédiation, avant une éventuelle sanction si celui-ci n'est pas instauré. De plus, la sanction financière est proportionnée à la gravité. Cette rédaction me semble concilier vos observations concernant les collectivités territoriales et notre obligation juridique de suivre l'avis du Conseil d'État.

M. Éric Bothorel, rapporteur général. Je crois en ce mécanisme, car il permet une graduation de la sanction et tient compte des spécificités des collectivités.

Vous avez souligné, madame la rapporteure, que la sanction ultime pour les élus était réputationnelle, mais c'est vrai aussi pour les entreprises privées : il ne faut pas croire que, lorsqu'elles sont victimes de leaks, elles sont insensibles aux conséquences, lesquelles peuvent être bien plus dramatiques. Je pense à Camaïeu, dont le site web a été attaqué et rendu indisponible pendant plusieurs jours ; sans qu'aucune corrélation ait été formellement établie, la perte de chiffre d'affaires liée à l'indisponibilité du site marchand correspondait, peu ou prou, au montant demandé quelques mois plus tard pour assurer le plan de continuité de l'entreprise, laquelle a dû licencier plusieurs centaines de salariés – nous en connaissons tous, pour avoir fréquenté les boutiques de l'enseigne. Les conséquences ne sont donc pas réductibles à l'aspect financier pour les entreprises non plus.

De ce point de vue, la proposition du président me semble convenir et répondre aux attentes du Conseil d'État. Vous avez dit, madame Sebaihi, que les collectivités attaquées n'avaient pas besoin d'être, en plus, sanctionnées. Or le mécanisme proposé par le président vise non pas à sanctionner toutes les collectivités, mais seulement celles qui auraient commis des erreurs en matière de protection des données. Cette possibilité existe déjà dans notre droit depuis longtemps : l'administration est responsable en cas de dommages liés à des travaux publics. On pourrait imaginer, à l'extrême, qu'une cyberattaque soit de nature à nuire à des infrastructures publiques ou à des travaux publics ; dans ce cas, la collectivité serait condamnable et condamnée, ce que personne ici ne conteste. Par conséquent, le fait de placer les collectivités devant leurs responsabilités dans des cas de cyberattaque ou de cybermenace et de leur appliquer un régime de sanctions ne me choque pas – d'autant que le Conseil d'État considère qu'il n'y a aucune raison de les en exonérer.

La rédaction de l'amendement me paraît souple, juste et équilibrée : il n'y aura pas d'automaticité – le président Latombe a bien insisté sur le mot « peut » – et la sanction sera graduée, selon un calendrier qui restera à déterminer d'ici à la séance – le délai d'une semaine pouvant être perçu comme trop long ou pas assez.

Mme Anne Le Hénanff, rapporteure. Vous présentez cette proposition comme souple et modérée, mais je ne partage pas votre analyse.

L'idée de la remédiation, en revanche, me semble intéressante. C'est, de toute façon, ce que fera l'Anssi avec les collectivités qui auront failli, puisque la remédiation est l'étape qui suit la constatation d'un défaut de cybersécurité dans une collectivité. Et des acteurs désignés par l'Anssi ou disponibles dans les territoires seront présents pour les accompagner.

Par ailleurs, je ne suis pas favorable à ce qu'un montant figure dans la loi, qu'il s'agisse de 1 centime ou de 10 millions d'euros.

Avec tout le respect que je dois au Conseil d'État, il ne donne qu'un avis. En tant que parlementaires, nous sommes libres de faire la loi en tenant compte ou non de cet avis, qui n'est pas une injonction. En l'occurrence, je ne partage pas son analyse.

Je suis, je le répète, favorable à la remédiation ; l'étape suivante, si les mesures nécessaires n'ont toujours pas été mises en œuvre, est de rendre la situation publique – et je peux vous dire qu'une publication dans le journal *Ouest France* un lundi matin est aussi terrible qu'une amende de 5 millions d'euros !

Pour toutes ces raisons, et bien que je comprenne la démarche, je reste défavorable à ces amendements identiques.

M. Aurélien Lopez-Liguori (RN). Si aucun mécanisme de sanctions n'est prévu pour les opérateurs publics, le niveau de cybersécurité pour les données stockées risque d'y être moins bon que chez les opérateurs privés ; cela créerait un fait discriminant – comme entre zones rurales et zones urbaines en raison du seuil de 30 000 habitants.

Je suis d'accord avec Mme Le Hénanff pour trouver délicat le fait d'annoncer, de manière sèche, un montant de sanctions plafonné à 10 millions, sans que l'on puisse fixer une assiette ni faire de différence entre les collectivités, les SEM – sociétés d'économie mixte – ou les agences publiques. Le délai d'une semaine me semble aussi trop court. L'idée d'une sanction réputationnelle par la publication dans la presse est bonne, mais elle n'aura d'effets que sur les élus, tandis que les agences de l'État et les administrations centrales ne seront pas concernées.

Il serait utile de réunir un groupe de travail transpartisan d'ici à l'examen du texte en séance, afin de trouver ensemble une rédaction acceptable – pour l'instant, aucune ne semble bonne.

Mme Marina Ferrari (Dem). Je ne dirai pas mieux.

Certes, il existe déjà des cas dans lesquels les collectivités peuvent se voir infliger des pénalités, comme en matière de logements sociaux en vertu de la loi relative à la solidarité et au renouvellement urbains. Toutefois, les délais sont alors beaucoup plus longs, puisqu'il faut prendre le temps d'évaluer la livraison des opérations, d'établir un constat de carence, etc. Dans le cas présent, le délai d'une semaine pour mettre en place un plan de remédiation me semble bien trop court.

Par ailleurs, le montant de 10 millions d'euros est de nature à affoler les collectivités – même si j'ai bien noté qu'il s'agit d'une simple possibilité donnée à la commission des sanctions. Et pourquoi fixer un montant alors qu'on ne sait pas sur quoi le fonder ?

Je ne soutiendrai donc pas ces amendements. En revanche, je souscris à la proposition d'y travailler ensemble afin de parvenir à une rédaction équilibrée et acceptable pour tout le monde.

Mme Catherine Hervieu (EcoS). L'amendement du président Latombe envoie un signal de défiance aux collectivités, aux élus et aux services. Nul doute que, de toute façon, les collectivités concernées se saisiront du sujet sans attendre la promulgation de la loi ; les cyberattaques dont elles sont victimes sont déjà relayées par les réseaux d'élus, qui ont bien compris la nécessité de contribuer à la sécurité globale du pays.

Les collectivités, rappelons-le, votent des budgets à l'équilibre, mais doivent aussi contribuer à l'effort de redressement des comptes publics ; leur imposer des sanctions financières dans ce contexte, c'est en rajouter encore.

Enfin, les préfets, qui sont en relation avec les élus locaux et les collectivités, seront des relais pour les aider, en cas de difficultés, à appliquer la loi.

Pour toutes ces raisons, nous ne voterons pas ces amendements.

M. Éric Bothorel, rapporteur général. Il se passe des choses dans notre pays, en dehors de ces murs. J'entends ce qui se dit. Je voterai l'amendement de mon collègue président, mais je vais retirer le mien.

Je rebondis sur la proposition de réunir ceux qui, de bonne foi, sont prêts à travailler ensemble. J'entends aussi qu'on puisse avoir des convictions suffisamment fortes pour faire de l'exonération des collectivités un totem ; je ne ferai donc pas perdre de temps à ceux qui ne veulent pas participer à trouver une ligne de crête permettant de répondre à l'avis du Conseil d'État – qui reste un avis. Néanmoins, nous renverrions une bonne image des travaux parlementaires. Par conséquent, si d'aventure l'amendement du président n'était pas adopté, je vous propose de nous retrouver avant l'examen du texte en séance, dont la date n'est pas encore connue, et de travailler ensemble à une rédaction acceptable par tous sur ce point particulier.

L'amendement CS516 est ***retiré****.*

La commission ***rejette*** *l'amendement CS417.*

Amendements identiques CS512 de M. Éric Bothorel et CS419 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il s'agit de mettre l'article 37 du projet de loi en cohérence avec le changement de terminologie par rapport à la directive, en permettant à la commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense de statuer sur les manquements des acteurs aux dispositions qui leur sont applicables.

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

Amendement CS160 de Mme Marina Ferrari

Mme Marina Ferrari (Dem). De même que le texte prévoit le non-cumul des amendes administratives infligées par la Cnil et de celles de la commission des sanctions, cet amendement vise à interdire le cumul des sanctions au titre des directives REC (résilience des entités critiques) et NIS 2.

Mme Anne Le Hénanff, rapporteure. Je comprends l'intention. Nous avions posé cette question à M. Vincent Strubel, directeur général de l'Anssi, lors de son audition : il a indiqué qu'il n'y aurait pas de cumul des sanctions. C'est pourquoi je vous invite à retirer votre amendement.

L'amendement CS160 est ***retiré****.*

*La commission **adopte** l'amendement rédactionnel CS420 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS513 de M. Éric Bothorel et CS421 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. L'objectif de cet amendement est d'appliquer le règlement européen dit CRA (Cyber Resilience Act), 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. Il tire les conséquences des modifications proposées à l'article 26.

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

Amendements identiques CS514 de M. Éric Bothorel et CS422 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il s'agit de mettre le texte en conformité avec la directive NIS 2, qui ne conditionne pas l'interdiction d'exercer pour les dirigeants des entités essentielles à la persistance d'un manquement malgré l'imposition d'amendes pécuniaires.

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

*La commission **adopte** l'article 37 **modifié**.*

Après l'article 37

Amendements identiques CS517 de M. Éric Bothorel et CS423 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Nous souhaitons permettre à l'Anssi d'autoriser les organismes d'évaluation à évaluer la conformité à des exigences de cybersécurité et à délivrer des certificats de conformité en confiant au cas par cas, dans les schémas de certification, l'activité de certification à des organismes d'évaluation de la conformité.

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

CHAPITRE IV
Dispositions diverses d'adaptation

Article 38 : (art. 30 et 35 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique) *Alléger le contrôle des biens de cryptologie*

Amendement de suppression CS424 de M. Philippe Latombe

M. le président Philippe Latombe. L'article 38 n'a pas pour objet de transposer une disposition de la directive NIS 2. Or on nous explique depuis le début de l'examen du projet de loi qu'il faut s'en tenir au texte de base et ne pas faire de surtransposition ni utiliser ce véhicule pour autre chose.

Mme Anne Le Hénanff, rapporteure. C'est vrai que la présence de cet article me place dans une position difficile, puisque j'explique depuis le début qu'il ne faut pas surtransposer et se borner à transposer les stipulations de la directive NIS 2. Je dérogerai néanmoins à cette règle, même si je regrette que cet article, tout comme les articles 41 et 42, ait été inséré dans le titre II du projet de loi alors qu'il ne transpose pas la directive NIS 2 – il eût été préférable de regrouper ces articles dans un titre spécifique.

Cependant, les enjeux de simplification de la procédure d'exportation des biens de cryptologie sont essentiels et il ne me semble pas opportun de supprimer purement et simplement ces articles. C'est pourquoi je suis défavorable à votre amendement.

M. Éric Bothorel, rapporteur général. Ce débat montre qu'il est inconfortable d'examiner un texte en l'absence du gouvernement. Il est néanmoins essentiel que soient maintenus les articles 38, 41 et 42 relatifs au brouillage et aux réseaux. Mieux vaudrait débattre de la suppression de ces articles lors de l'examen en séance, en présence du gouvernement. C'est pourquoi je vous invite à retirer vos amendements ; à défaut, avis défavorable.

M. le président Philippe Latombe. Je le maintiendrai pour la simple et bonne raison que, depuis le début de l'examen du texte, chaque fois que nous proposons d'y intégrer de nouvelles notions – la souveraineté, la dépendance –, on nous répond que ce projet de loi n'est pas le bon véhicule et qu'il ne faut pas mélanger les choses. Or, dans ce cas précis, nous mélangeons les choses. Si nous voulons être cohérents jusqu'au bout, nous devons supprimer les articles 38, 41 et 42 qui n'ont rien à voir avec la directive NIS 2.

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

Amendements identiques CS518 de M. Éric Bothorel et CS425 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Ces amendements, essentiellement rédactionnels, visent à améliorer la lisibilité du dispositif pour les destinataires de l'obligation de déclaration des moyens de cryptologie.

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

*Elle **adopte** l'article 38 **modifié**.*

Article 39 : (articles L. 2321-2-1 et L. 2321-3 du code de la défense, articles L. 33-1, L. 45, L. 45 3, L. 45-4, L. 45-5 et L. 45-8 du code des postes et des communications électroniques, titre I[er] de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité [supprimés], articles 1[er], 9, 12 et 14 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives) *Abrogation de la transposition de la directive NIS 1 et simplification du cadre réglementaire*

*La commission **adopte** successivement les amendements rédactionnels identiques CS519 de M. Éric Bothorel, rapporteur général, et CS426 de Mme Anne Le Hénanff, rapporteure, ainsi que l'amendement rédactionnel CS428 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS520 de M. Éric Bothorel et CS427 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Ils visent à assurer la coordination avec l'amendement qui définit les agents agissant pour le compte des bureaux d'enregistrement et supprime en conséquence le renvoi à un décret en Conseil d'État qui devait prévoir cette définition.

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

*Puis elle **adopte** les amendements de coordination identiques CS521 de M. Éric Bothorel, rapporteur général, et CS429 de Mme Anne Le Hénanff, rapporteure.*

*Elle **adopte** l'article 39 **modifié**.*

Article 40 : (article 57 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 24 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 16 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives) *Mesures applicables à l'outre-mer pour les territoires régis par le principe de spécialité législative*

*La commission **adopte** successivement les amendements rédactionnels CS430, CS431 et CS432 de Mme Anne Le Hénanff, rapporteure.*

*Elle **adopte** l'article 40 **modifié**.*

CHAPITRE V
Dispositions relatives aux communications électroniques

Article 41 : (article L. 39-1 du code des postes et des communications électroniques) *Renforcement des sanctions pénales pour améliorer la lutte contre les brouillages*

Amendement de suppression CS433 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à supprimer cet article, qui n'a pas sa place dans le cadre de la transposition de la directive NIS 2. Comme je l'ai déjà indiqué, l'ajout d'un certain nombre de notions a été écarté au prétexte d'éviter une surtransposition. Or cet article est précisément une mesure de surtransposition.

Mme Anne Le Hénanff, rapporteure. Cet article n'opère pas de surtransposition de la directive NIS 2 puisqu'il ne relève pas de la directive. En revanche, il est mal placé.

Cet article est utile : la lutte contre les brouillages est indispensable. En effet, ils se multiplient et peuvent avoir des conséquences graves pour la sécurité des individus ainsi que la sûreté d'infrastructures, de services et d'industries stratégiques. Ces risques de brouillage peuvent également concerner les fréquences utilisées par les armées. Protéger le spectre contre les brouillages, c'est assurer la résilience de l'ensemble des services y étant associés. S'il ne concerne pas la cyber-résilience, cet article vise néanmoins à renforcer la résilience de la nation.

M. Éric Bothorel, rapporteur général. À l'heure où l'agresseur d'un pays voisin utilise ce type de technologie, nous avons besoin de cette disposition pour nous protéger. Il serait maladroit de se passer de ce véhicule. J'insiste pour que cet article soit adopté.

M. le président Philippe Latombe. On nous a expliqué qu'une mesure relative aux sondes avait plutôt sa place dans la LPM. De la même manière, l'article 41 relève davantage de la LPM.

M. Aurélien Lopez-Liguori (RN). Depuis le début de l'examen du texte, lorsqu'on propose d'ajouter une nouvelle notion liée à la cybersécurité – par exemple la souveraineté ou la commande publique –, on nous explique que cela reviendrait à surtransposer. En outre, lorsqu'on souhaite faire notre travail de législateur en inscrivant des sujets urgents dans ce véhicule, on nous répond que ce n'est pas possible.

Nous ne voterons pas la suppression de cet article car nous sommes favorables au renforcement des sanctions pénales pour lutter contre les brouillages, mais ce sujet n'a rien à faire ici puisqu'il ne relève pas de la directive. Si cet amendement est adopté, comment maintiendrez-vous votre argument de la surtransposition lorsqu'en séance nous débattrons de nouveau des sondes, de la commande publique ou encore de la souveraineté, qui ont un lien direct avec la cybersécurité ? Votre position est décidément inconfortable.

M. Éric Bothorel, rapporteur général. Je ne manque pas de souplesse. Je rappelle qu'à l'article 5 *bis,* plusieurs amendements, adoptés contre l'avis du rapporteur général, ont introduit des mesures techniques ou plus générales qui enrichissent le texte. Or nous discutons d'articles techniques qui portent sur des sujets précis ; ils ne sauraient être placés sur le même plan que l'introduction de concepts non définis tels que l'autonomie stratégique ou la souveraineté. Convenez que nous ne parlons pas des mêmes objets.

S'agissant des sondes, j'ai insisté sur le fait que ce sujet n'était pas clos et que nous devions le travailler de nouveau d'ici à la séance. Ce qui est inconfortable, c'est l'absence de l'exécutif, qui ne peut pas indiquer les raisons pour lesquelles il souhaite particulièrement le maintien de ces articles. Il serait donc raisonnable que nous débattions de cette question en séance, avec le gouvernement. D'ici là, la suppression de ces articles serait maladroite.

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

La commission ***adopte*** *les amendements rédactionnels CS434, CS435, CS436, CS437, CS438 et CS439 de Mme Anne Le Hénanff, rapporteure.*

Elle ***adopte*** *l'article 41* ***modifié****.*

Article 42 : (articles L. 97-2 et L. 97-4 du code des postes et des communications électroniques) *Renforcement des conditions d'accès à une assignation de fréquences déposée par la France auprès de l'UIT*

Amendement de suppression CS440 de M. Philippe Latombe

M. Éric Bothorel, rapporteur général. Dans un souci de clarification, d'ici à la séance, il pourrait être proposé de créer un titre IV – sans pour autant ouvrir une liste à la Prévert – regroupant les articles 38, 41 et 42, puisqu'ils comportent des éléments absents de la directive NIS 2.

Mme Anne Le Hénanff, rapporteure. Avis défavorable, pour les raisons évoquées à l'occasion de l'examen des amendements de suppression des articles 38 et 41.

M. le président Philippe Latombe. Il faudra déposer en séance un amendement en ce sens.

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

Puis elle ***adopte*** *les amendements rédactionnels CS441, CS442, CS443, CS444 et CS445 de Mme Anne Le Hénanff, rapporteure.*

Elle ***adopte*** *l'article 42* ***modifié****.*

La réunion est suspendue de quinze heures trente à quinze heures trente-cinq.

TITRE III
RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DU SECTEUR FINANCIER

CHAPITRE IER
Dispositions modifiant le code monétaire et financier

Avant l'article 43 A

Amendement CS176 de Mme Sabrina Sebaihi

Mme Sabrina Sebaihi (EcoS). Il vise à créer un comité national d'observation des risques cyber dans le secteur bancaire, financier et assurantiel. L'objectif est de suivre l'évolution des menaces, d'évaluer la mise en œuvre des obligations en matière de cybersécurité et surtout d'éviter que les coûts ne soient injustement répercutés sur les usagers.

Ce comité associerait des représentants des établissements bancaires, financiers et assurantiels, des autorités de régulation, de l'Anssi et des consommateurs, sans coût supplémentaire puisque ses membres siégeraient à titre gratuit.

Il ne s'agit pas d'alourdir le système mais plutôt de renforcer la confiance et la transparence d'un secteur exposé à des risques croissants.

M. Mickaël Bouloux, rapporteur pour le titre III. Je ne suis pas convaincu qu'il soit nécessaire de créer une instance pour s'assurer du respect de la directive NIS 2 et du règlement Dora par les entités financières. C'est le rôle de l'Anssi et des autorités compétentes respectives, notamment l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF).

Par ailleurs, ce comité ne pourrait garantir l'absence de répercussion des coûts pour les consommateurs.

Je vous invite à retirer votre amendement ; à défaut, avis défavorable.

M. Éric Bothorel, rapporteur général. Même avis.

Je profite de l'occasion pour vous indiquer que sur les 170 amendements adoptés avant la reprise de nos travaux à 14 heures, 16 avaient été déposés le groupe Démocrates, 1 par le groupe socialiste, 1 par le groupe Droite républicaine, 11 par le groupe écologiste, 41 par le groupe EPR, 1 par le groupe GDR, 88 par le groupe Horizons, 9 par le groupe La France insoumise, 1 par le groupe LIOT et 1 par le groupe Rassemblement national. Notre commission travaille bien.

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

Article 43 A (nouveau) : (articles L. 141-10 et L. 612-24-1 [nouveaux] du code monétaire et financier) *Désignation de la Banque de France et de l'Autorité de contrôle prudentiel et de résolution comme autorités compétentes dans le cas où une entité financière est assujettie à plusieurs autorités de supervision*

Amendements CS242 de M. Mickaël Bouloux et CS263 de M. Paul Midy, amendements identiques CS109 de M. Philippe Latombe, CS522 de M. Éric Bothorel et CS531 de M. Mickaël Bouloux (discussion commune)

M. Mickaël Bouloux, rapporteur. L'article 19 du règlement Dora prévoit que les entités financières déclarent à l'une des autorités compétentes visées à l'article 46 les incidents majeurs liés aux technologies de l'information et de la communication (TIC). Elles peuvent également notifier, à titre volontaire, les cybermenaces importantes à l'autorité compétente lorsqu'elles estiment que la menace peut concerner le système financier, les utilisateurs de services ou les clients.

Dans un objectif de simplification, le Sénat a décidé que les déclarations d'incident des entités financières ne seraient plus transmises qu'à la Banque de France, l'ACPR ou l'AMF, selon l'autorité concernée. Or il est nécessaire que l'Anssi soit également destinataire de ces déclarations, notamment en cas de contagion.

Je vous propose de soutenir mon amendement qui permettrait de préserver le rôle primordial de l'Anssi dans la gestion des cybermenaces, y compris de celles affectant les entités financières.

Si cet amendement était adopté, d'une part, il ferait tomber les autres amendements en discussion commune, d'autre part, il permettrait de supprimer l'article 45 *bis*, qui serait intégré au présent article.

M. Paul Midy (EPR). L'amendement CS263 vise à désigner l'ACPR comme autorité compétente chargée de recevoir les déclarations d'incident et les notifications de cybermenaces de la part des entités financières soumises à la surveillance des autorités compétentes.

Les entités assujetties à NIS 2 devront transmettre ces déclarations à l'Anssi ; il ne s'agira que d'une simple faculté pour les autres entités. En clair, cet amendement vise à préciser le rôle des différents acteurs.

M. Éric Bothorel, rapporteur général. Je retire l'amendement CS522.

M. Mickaël Bouloux, rapporteur. L'amendement CS531 est un amendement de repli.

Le Sénat a choisi de désigner l'ACPR comme unique destinataire des déclarations d'incident majeur lié aux TIC et des notifications volontaires de cybermenace, en application du règlement Dora. Il ressort des auditions qu'il est absolument nécessaire que l'Anssi soit également destinataire de ces déclarations, comme le prévoit par ailleurs la directive NIS 2, puisque la plupart des entités financières sont des entités importantes ou essentielles.

À la lecture des amendements, je constate que nous sommes tous d'accord sur ce point. Plusieurs amendements – celui de M. Midy et les amendements ultérieurs CS48 et CS161 – prévoient bien l'information de l'Anssi mais n'instaurent pas un guichet unique ou, à tout le moins, un formulaire unique. Les entités financières y sont pourtant attachées au nom de la simplification administrative.

L'amendement CS242 tend simplement à ce que les démarches des entités financières prévues au titre de Dora et de NIS 2 soient accomplies auprès de l'Anssi et de leur autorité de supervision au moyen d'un document unique. C'est aussi ce que propose le président, qui a déposé deux amendements distincts : l'un concernant l'ACPR, l'autre l'AMF à l'article 45 *bis*. Il me semble que la rédaction de l'amendement CS242 est meilleure puisqu'elle englobe toutes les autorités de supervision ; je vous invite à le voter.

M. Éric Bothorel, rapporteur général. J'invite le rapporteur et le président à retirer leurs amendements au profit de celui de M. Midy ; à défaut, j'émettrai un avis défavorable.

L'amendement CS242 impose par la loi une modalité purement technique : l'utilisation d'un document unique. Or ce sujet relève du domaine réglementaire.

L'ACPR est l'autorité de référence des entités financières, mais l'amendement fusionne les régimes issus de Dora et de NIS 2 sans en préciser l'articulation, au risque de brouiller les responsabilités et de créer une insécurité juridique.

Par ailleurs, le champ me paraît trop large. La mention de « tout incident ayant un impact important » excède le périmètre financier.

En outre, l'amendement supprime une distinction essentielle que prévoient le règlement Dora et la directive NIS 2 : la notification obligatoire s'imposant aux entités soumises à ces deux réglementations et la notification facultative s'agissant des cybermenaces.

Pour ces raisons, j'émets un avis défavorable sur l'amendement CS242 malgré la qualité du travail accompli.

S'agissant des amendements identiques CS109 et CS531, ils ne couvrent pas les outre-mer. Je vous invite donc à voter l'amendement CS263.

M. Denis Masséglia (EPR). M. le rapporteur pense que son amendement est le mieux rédigé ; nous pensons que c'est le nôtre.

*La commission **rejette** l'amendement CS242.*

*Elle **adopte** l'amendement CS263 et l'article 43 A est **ainsi rédigé** ; en conséquence, les amendements identiques **tombent**, ainsi que l'amendement CS48.*

Après l'article 43 A

*L'amendement CS161 de Mme Marina Ferrari est **retiré**.*

Article 43 : (art. L. 314-1 du code monétaire et financier) *Modification de la définition des prestataires de services techniques*

*La commission **adopte** l'article 43 **non modifié**.*

Article 44 : (art. L. 420-3 du code monétaire et financier) *Maintien de la résilience opérationnelle des gestionnaires de plates-formes de négociation*

La commission ***adopte*** *l'amendement rédactionnel CS243 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 44* ***modifié****.*

Article 45 : (art. L. 421-4 et L. 421-11 du code monétaire et financier) *Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché*

La commission ***adopte*** *l'article 45* ***non modifié****.*

Article 45 ***bis*** **(nouveau)** : (art. L. 54-10-7 et L. 421-11-1 [nouveau] du code monétaire et financier) *Désignation de l'Autorité des marchés financiers comme autorité compétente dans le cas où une entreprise de marché ou un prestataire de services pour crypto-actifs est assujetti à plusieurs autorités de supervision*

Amendement de suppression CS244 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. Il n'a plus lieu d'être puisque l'amendement CS242 n'a pas été adopté.

L'amendement est ***retiré****.*

Amendements identiques CS110 de M. Philippe Latombe, CS523 de M. Éric Bothorel et CS533 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. Cet amendement de repli vise à mettre le texte en cohérence avec la disposition adoptée à l'article 43 A.

La commission ***adopte*** *les amendements et l'article 45* bis *est* ***ainsi rédigé****.*

Après l'article 45 ***bis***

Amendement CS47 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons développer le partage d'informations entre les entités financières et les agences chargées de la gestion de leurs incidents de cybersécurité en systématisant également la notification de cybermenaces lorsque celles-ci sont identifiées par les entités financières. Le règlement Dora ne prévoit qu'une notification volontaire ; en la généralisant, on préviendrait d'éventuels incidents avec la détection en amont des principales cybermenaces pesant sur les entités financières.

M. Mickaël Bouloux, rapporteur. Compte tenu des amendements adoptés aux articles 43 A et 45 *bis*, celui-ci n'est plus opportun. Je vous invite à le retirer.

L'amendement est ***retiré****.*

Article 46 : (art. L. 511-41-1-B du code monétaire et financier) *Références aux risques liés aux technologies de l'information et de la communication au sein des dispositifs de gestion des risques des établissements de crédit et des sociétés de financement*

La commission ***adopte*** *l'amendement rédactionnel CS245 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 46* ***modifié****.*

Article 47 : (art. L. 511-55 du code monétaire et financier) *Référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement*

La commission ***adopte*** *l'article 47* ***non modifié****.*

Article 48 : (art. L. 521-9 du code monétaire et financier) *Obligations des prestataires de services de paiement en matière de gestion du risque lié aux technologies de l'information et de la communication*

La commission ***adopte*** *l'article 48* ***non modifié****.*

Article 49 : (art. L. 521-10 du code monétaire et financier) *Modification de la liste des prestataires de services de paiement soumis à une obligation de notification des incidents opérationnels ou de sécurité majeur*

Amendement CS246 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. Amendement rédactionnel.

M. Éric Bothorel, rapporteur général. Il n'est pas tout à fait rédactionnel : remplacer « notification » par « déclaration » n'est pas neutre. L'article 19 du règlement Dora utilise expressément le terme « notification ». Introduire une autre terminologie en droit national risquerait de créer une divergence avec le texte européen, source d'insécurité juridique pour les entités et de difficultés d'interprétation pour les juges et autorités de supervision. Cela nuirait à l'harmonisation recherchée par Dora. Avis défavorable.

L'amendement est ***retiré****.*

La commission ***adopte*** *l'article 49* ***non modifié****.*

Article 49 ***bis*** **(nouveau)** : (art. L. 532-50 du code monétaire et financier) *Extension de l'application du règlement Dora aux succursales d'entreprises d'investissement de pays tiers*

La commission ***adopte*** *l'amendement rédactionnel CS247 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 49* bis ***modifié****.*

Article 50 : (art. L. 533-2 du code monétaire et financier) *Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement*

La commission ***adopte*** *l'article 50* ***non modifié****.*

Article 51 : (art. L. 533-10 du code monétaire et financier) *Systèmes de technologies de l'information et de la communication et dispositifs de contrôle des prestataires de services d'investissement*

La commission ***adopte*** *l'amendement rédactionnel CS248 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 51* ***modifié****.*

Article 52 : (art. L.533-10-4 du code monétaire et financier) *Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique*

La commission ***adopte*** *l'amendement rédactionnel CS249 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 52* ***modifié****.*

Article 53 (supprimé) : (art. L.612-24 du code monétaire et financier) *Référence aux prestataires informatiques critiques au sein des tiers auxquels l'Autorité de contrôle prudentiel et de résolution peut demander toute information*

La commission ***maintient la suppression de*** *l'article 53.*

Article 54 : (art. L. 613-38 du code monétaire et financier) *Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement*

La commission ***adopte*** *l'amendement rédactionnel CS250 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 54* ***modifié****.*

Article 55 : (art. L. 631-1 du code monétaire et financier) *Extension de la liste des autorités habilitées à échanger des informations*

La commission ***adopte*** *l'amendement rédactionnel CS251 de M. Mickaël Bouloux, rapporteur.*

Elle ***adopte*** *l'article 55* ***modifié****.*

Article 56 : (art. L. 712-7, L. 752-10, L.753-10, L. 754-8, L. 761-1, L. 762-3, L. 763-3, L. 764-3, L. 762 4, L. 763 4, L. 764-4, L. 771-1, L. 781-1, L.773-5, L. 774-5, L. 775-5, L. 773-6, L. 774-6, L. 775-6, L. 773-21, L. 774-21, L. 775-15, L. 773-30, L. 774-30, L.775-24, L. 783 2, L. 784 2, L. 785-2, L. 783-4, L. 784-4, L. 785-4, L. 783-13, L. 784-13 et L. 785 -12 du code monétaire et financier) *Adaptations pour rendre applicables en outre-mer les modifications du code monétaire et financier prévues par le présent projet de loi*

Amendement CS252 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. Cet amendement de coordination tient compte de plusieurs modifications du Sénat et corrige des erreurs de référence.

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

Elle ***adopte*** *l'article 56* ***modifié****.*

CHAPITRE II
Dispositions modifiant le code des assurances

Article 57 : (art. L. 354-1 du code des assurances) *Nouvelles obligations pour les entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information*

*La commission **adopte** l'amendement rédactionnel CS253 de M. Mickaël Bouloux, rapporteur.*

*Elle **adopte** l'article 57 **modifié**.*

Article 58 : (art. L. 356-18 du code des assurances) *Extension aux groupes d'assurance des nouvelles obligations de gouvernance des risques liés à l'utilisation des systèmes d'information*

*La commission **adopte** l'amendement rédactionnel CS254 de M. Mickaël Bouloux, rapporteur.*

*Elle **adopte** l'article 58 **modifié**.*

Article 58 *bis* (nouveau) : (art. L. 121-8 du code des assurances) *Inversion de la charge de la preuve pour les cyberattaques*

Amendements identiques CS524 de M. Éric Bothorel et CS255 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. Le Sénat a adopté un amendement qui vise à inverser la charge de la preuve vis-à-vis des assurances en cas de cyberattaque, mais la rédaction retenue va à l'encontre de l'objectif recherché car elle prévoit qu'il appartient à l'assureur de prouver qu'un sinistre résulte de la guerre civile, d'émeutes, de mouvements populaires ou d'attaques informatiques précisément lorsque ces risques ne sont pas couverts par le contrat d'assurance.

Je vous propose donc un amendement rédigé en lien avec France Assureurs, l'Anssi et la direction générale du Trésor, qui prévoit qu'en cas de sinistre résultant d'une atteinte à un système de traitement automatisé de données, l'assureur doit prouver qu'il résulte d'une guerre étrangère pour ne pas avoir à l'indemniser puisque les pertes et dommages occasionnés par une guerre étrangère ne sont pas couverts par les polices d'assurance.

M. le président Philippe Latombe. À titre d'information, je vous signale que l'adoption de ces amendements ferait tomber l'amendement CS241 de Mme Sabrina Sebaihi.

*La commission **adopte** les amendements identiques et l'article est **ainsi rédigé** ; en conséquence, l'amendement CS241 **tombe**.*

CHAPITRE III
Dispositions modifiant le code de la mutualité

Article 59 : (art. L. 211-12 du code de la mutualité) *Nouvelles obligations pour les unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information*

*La commission **adopte** l'amendement rédactionnel CS256 de M. Mickaël Bouloux, rapporteur.*

*Elle **adopte** l'article 59 **modifié**.*

Article 60 : (art. L. 212-1 du code de la mutualité) *Suppression de dispositions redondantes dans le code de la mutualité*

Amendement CS257 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. Amendement rédactionnel.

M. Éric Bothorel, rapporteur général. Il est satisfait : le projet de loi initial comporte déjà la modification pertinente. En outre, il mélange des dispositions issues de deux codes distincts – l'article L. 354-1 du code des assurances et l'article L. 212-1 du code de la mutualité –, ce qui rend la rédaction inopérante et juridiquement incohérente. Avis défavorable.

*L'amendement est **retiré**.*

*La commission **adopte** l'article 60 **non modifié**.*

CHAPITRE IV
Dispositions modifiant le code de la sécurité sociale

Article 61 : (art. L. 931 7 du code de la sécurité sociale) *Nouvelles obligations pour les institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information*

*La commission **adopte** l'amendement rédactionnel CS258 de M. Mickaël Bouloux, rapporteur.*

*Elle **adopte** l'article 61 **modifié**.*

CHAPITRE V
Dispositions finales

Article 62 A (nouveau) : *Absence de double assujettissement à Dora et NIS 2*

Amendement CS525 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Il vise à corriger une erreur de référence et à étendre explicitement l'application de l'article aux collectivités ultramarines.

M. Mickaël Bouloux, rapporteur. Si l'amendement CS242 avait été adopté, celui-ci n'aurait pas été nécessaire mais comme ce n'est pas le cas, j'émets un avis favorable.

*La commission **adopte** l'amendement CS525 ; en conséquence, l'amendement CS259 **tombe**.*

*La commission **adopte** l'article 62 A **modifié**.*

Après l'article 62 A

Amendements CS260 et CS473 de M. Mickaël Bouloux

M. Mickaël Bouloux, rapporteur. L'amendement CS260 porte sur un sujet qui nous a été signalé lors des auditions et qui avait échappé au Sénat. Le nouveau cadre de gestion oblige les entités financières à prévoir des obligations plus strictes dans la contractualisation avec leurs prestataires de services de TIC. Dès lors, ces derniers pourraient se voir soumettre à des audits pour vérifier la conformité de leurs prestations de services avec les exigences contractuelles de leurs clients, qui sont eux-mêmes soumis au règlement Dora. On peut donc craindre qu'elles aient à communiquer des données sensibles à des cabinets d'audit étrangers, voire qu'elles fassent l'objet d'enquêtes intrusives de leur part, quand bien même ils le feraient pour le compte d'une entité financière française.

Certes, la loi du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères interdit déjà de communiquer des informations de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public. Cependant, un système d'agrément, comme proposé dans cet amendement, permettrait d'éviter ces risques et faciliterait le travail des prestataires tiers de services TIC.

C'est pourquoi je propose d'établir une liste d'auditeurs approuvés par une autorité indépendante telle que l'Anssi ou l'ACPR pour réaliser, à la demande des entités financières, les inspections prévues au chapitre V du règlement Dora relatif à la gestion des risques liés aux prestataires tiers de services TIC.

L'amendement CS473, est un amendement de repli. À défaut d'une liste fermée et d'un agrément, il est proposé un référentiel des bonnes pratiques et un annuaire des auditeurs.

M. Éric Bothorel, rapporteur général. Je comprends l'intention de protéger les prestataires français contre les risques d'audits intrusifs conduits par des cabinets étrangers en instaurant un filtre souverain. Cela permettrait aussi de donner de la visibilité aux entités financières sur les acteurs autorisés à réaliser ce type d'audit. Toutefois, votre amendement CS260 pose plusieurs difficultés. Il va au-delà de ce que prévoit Dora et risque donc de constituer une surtransposition, fragilisant la conformité au droit européen. Il introduit une barrière à l'entrée sur le marché des services d'audit TIC avec un risque de distorsion concurrentielle. Il alourdit la mise en œuvre opérationnelle et pourrait restreindre excessivement l'offre disponible pour les entités financières. J'en demande donc le retrait. À défaut, j'émettrais un avis défavorable.

J'ai le même avis sur l'amendement CS473, mais je veux bien participer à des travaux de réflexion visant à en proposer une nouvelle rédaction en séance. Le risque de surtransposition existe aussi pour cet amendement de repli : dans son article 28, le règlement prévoit déjà un cadre détaillé pour la gestion des partenaires TIC, y compris pour les audits, et n'impose pas un tel annuaire national. Même non exclusif, l'annuaire pourrait devenir en pratique une liste fermée et dissuader le recours à d'autres auditeurs, en contradiction avec le droit européen de la concurrence et de la libre prestation de services ; il créerait un risque de distorsion de concurrence. Enfin, le risque de complexité opérationnelle subsiste : les entités financières seraient confrontées à des référentiels nationaux qui viendraient se superposer aux standards européens.

Il me semble que la loi de « blocage » de 1968 protège déjà contre les ingérences étrangères. Il n'est donc pas nécessaire d'aller plus loin dans le droit interne mais encore une fois, je peux m'engager à travailler avec vous sur ce point d'ici à la séance.

M. Mickaël Bouloux, rapporteur. Je retire l'amendement CS260, mais je maintiens l'amendement CS473.

M. Aurélien Lopez-Liguori (RN). Il est dommage que vous retiriez ce très bon amendement. La direction générale de la sécurité intérieure (DGSI) a donné l'alerte concernant les cabinets d'audits étrangers – en particulier les Big Four que sont Deloitte, EY, KPMG et PwC – qui sont soumis à l'application extraterritoriale de législations étrangères. Il est arrivé à plusieurs reprises que des entreprises fassent l'objet d'offres publics d'achat (OPA) agressives de la part de concurrentes américaines qui avaient bénéficié d'informations confidentielles fuitant à la suite de tels audits. Il est donc très pertinent de réserver à des entreprises européennes, soumises au droit de l'UE, la possibilité de faire ces audits.

Le rapporteur général redoute que l'amendement crée une distorsion de concurrence. En effet, mais celle-ci va être créée entre acteurs européens et extra-européens, ce qui est une très bonne chose ! Nous sommes des parlementaires français. Créer une distorsion de concurrence vis-à-vis d'acteurs extra-européens ne devrait pas nous poser de problèmes ni susciter en nous ces pudeurs de gazelle.

L'amendement CS260 est ***retiré****.*

La commission ***rejette*** *l'amendement CS473.*

Article 62 : *Dates d'application des dispositions du titre III*

Amendement CS46 de M. René Pilato, amendements identiques CS527 de M. Éric Bothorel et CS261 de M. Mickaël Bouloux, amendement CS262 de M. Mickaël Bouloux (discussion commune)

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons supprimer le report en 2030 de l'application des dispositions du présent projet de loi pour les sociétés de financement. En France, les sociétés de financement et les établissements de crédit sont soumis aux mêmes règles prudentielles, ce qui n'est pas le cas dans tous les pays européens. La directive Dora ne s'applique pas explicitement à ces sociétés. Les rapporteurs du texte au Sénat ont prétexté une supposée surtransposition pour repousser l'application de la directive à ces entités à 2030. Il convient toutefois de prendre en compte cette particularité du droit français : les sociétés de financement doivent donc être soumises aux mêmes règles prudentielles que les autres entités financières, et rien ne justifie le report en 2030 de l'application des dispositions du présent projet de loi.

M. Mickaël Bouloux, rapporteur. Mon amendement CS261 prévoit de revenir sur le délai accordé par le Sénat à toutes les sociétés de financement, y compris les plus grandes, pour se mettre en conformité avec les exigences prudentielles propres aux prestataires de services bancaires, édictée par le règlement Dora. Le projet de loi initial prévoyait une entrée en vigueur immédiate pour une dizaine de grandes sociétés de financement, dont la plus sensible est le Crédit Logement, qui se porte garant de prêts immobiliers de particuliers, et une entrée en application différée d'un an pour les sociétés de financement les plus petites, c'est-à-dire la grande majorité du secteur.

Le Sénat a voulu accorder à toutes, même les plus grandes, une entrée en application au 1er janvier 2030. Ce délai semble excessif au regard des enjeux en matière de résilience opérationnelle numérique. Je propose de rétablir un délai différencié : une entrée en vigueur immédiate pour les grandes sociétés de financement, et un report au 17 janvier 2027 – soit un an de plus que ce que prévoyait le projet de loi initial – pour les autres. C'est pourquoi j'émettrai un avis défavorable sur l'amendement CS46 qui ne fait aucune distinction en fonction de la taille des sociétés.

L'amendement de repli CS262 vise à retenir la date du 17 janvier 2027 pour toutes les sociétés de financement, même si je pense qu'il n'y a pas de raison de ne pas imposer une application immédiate aux plus importantes.

M. Éric Bothorel, rapporteur général. Comme le rapporteur, je demande le retrait de l'amendement CS46 au profit des amendements identiques.

L'amendement CS46 est ***retiré****.*

La commission ***adopte*** *les amendements identiques ; en conséquence, l'amendement CS262* ***tombe****.*

La commission ***adopte*** *l'amendement rédactionnel C526 de M. Éric Bothorel, rapporteur général.*

Elle ***adopte*** *l'article 62* ***modifié****.*

Après l'article 62

Amendement CS65 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons que le gouvernement remette au Parlement un rapport annuel sur la mise en œuvre de la stratégie nationale en matière de cybersécurité, qui précise les moyens humains, techniques et financiers mis à sa disposition pour l'exercice de ses missions de contrôle et d'audit. Ce rapport évaluera également les besoins à venir au regard de l'élargissement du périmètre des entités concernées par la présente loi. Il s'agit de s'assurer que les moyens alloués à l'Anssi seront suffisants, ce que ne permet pas ce projet de loi.

M. Éric Bothorel, rapporteur général. Avis défavorable.

Mme Anne Le Hénanff, rapporteure. Même si je ne crois pas souhaitable de demander des rapports trop nombreux, celui-ci pourrait avoir le mérite de mettre en évidence le manque de moyens de l'Anssi. J'y suis assez favorable.

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

Amendement CS83 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Dans leur rapport d'information sur la cyberdéfense, Bastien Lachaud et Alexandra Valetta Ardisson recommandent d'établir une carte des entreprises et des compétences critiques de la base industrielle et technologique de défense (BITD), puis un plan de sécurisation incluant les sous-traitants. En matière cyber, ils invitent à rendre le donneur d'ordres responsable de l'ensemble de la chaîne, afin de garantir une solidarité effective. Souvent, les sous-traitants sont les maillons les plus vulnérables : pour préserver l'ensemble des actifs stratégiques, il est vital de les protéger.

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

Amendement CS107 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Depuis une dizaine d'années, les satellites en orbite basse prolifèrent. Le spectre électromagnétique est une ressource naturelle rare et limitée, gérée par l'Union internationale des télécommunications (UIT). En France, les opérateurs passent par l'intermédiaire de l'Agence nationale des fréquences (ANFR) pour demander l'attribution d'une fréquence.

L'accélération des projets de mégaconstellation, dont celui de Starlink n'est qu'un exemple, s'accompagne de tentatives d'accaparer les couples spectres-orbites. Des milliers de demandes sont formulées chaque année. L'encombrement de l'orbite basse par les systèmes placés en coexistence forcés pose des problèmes désormais bien connus, en particulier les collisions en chaîne : le syndrome de Kessler soulève la question de la soutenabilité de ces activités.

L'amendement vise à obtenir un rapport relatif à l'allocation des fréquences afin d'établir un bilan des évolutions en cours et de leur incidence sur le développement de nos infrastructures en orbite et sur l'environnement spatial – on accorde beaucoup trop de licences.

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

Amendement CS85 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Il vise à obtenir un rapport sur l'état du réseau de l'Anssi dans les territoires ultramarins.

Lors des auditions, Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique pour Régions de France, nous a expliqué que l'accompagnement humain et financier et la résilience face aux attaques constituaient des sujets de grande préoccupation dans toutes les collectivités. Les territoires éloignés de l'Hexagone ne sont pas forcément armés pour résister aux cyberattaques. Il est essentiel d'établir un état des vulnérabilités pour déterminer comment y remédier.

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

Amendement CS63 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Nous devons impérativement allouer à l'Anssi les moyens suffisants pour faire appliquer les dispositions issues de la transposition de NIS 2. Cet amendement vise à obtenir un rapport établissant ceux qui lui seront nécessaires.

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

Amendement CS77 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Il vise à obtenir un rapport sur les moyens alloués aux collectivités territoriales pour combattre les menaces cyber.

Un rapport du cabinet de conseil Idate paru en novembre 2024 estime qu'elles devront dépenser 690 millions d'euros par an pour se mettre en conformité avec NIS 2, et 105 millions de plus pour embaucher et former le personnel qualifié.

Tout le monde pourra ainsi prendre conscience de la catastrophe budgétaire que le gouvernement provoque : il dépossède les collectivités de leurs moyens, puis les contraint à adopter des mesures essentielles pour leur cybersécurité, qu'elles ne peuvent plus assurer.

M. Éric Bothorel, rapporteur général. La commission des finances évalue les politiques publiques et contrôle l'action du gouvernement. Elle fait un excellent travail : elle pourra nous éclairer quant à la nécessité de soutenir les collectivités.

Vous êtes libre de parler d'austérité et de condamner la politique de soutien public. Cependant, nous disposons des moyens suffisants pour ne pas solliciter en permanence le gouvernement dans le but d'obtenir des éléments que nous pouvons nous-même établir.

Avis défavorable.

Mme Anne Le Hénanff, rapporteure. J'émets également un avis défavorable. Les collectivités décideront elles-mêmes du montant de l'investissement à consentir pour se mettre en conformité. Il serait difficile d'en décider depuis Paris. Le travail d'évaluation devra être mené, mais localement.

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

La commission ***adopte*** *l'ensemble du projet de loi* ***modifié****.*

La séance est levée à seize heures vingt.

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 mercredi 10 septembre 2025 à 14 heures

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