N° 1779

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 10 septembre 2025.

RAPPORT

FAIT

AU NOM DE LA COMMISSION SPÉCIALE [1] CHARGÉE D'EXAMINER LE 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),

PAR M. ÉRIC BOTHOREL
Rapporteur général,

ET

M. MICKAËL BOULOUX, MMES CATHERINE HERVIEU ET ANNE LE HÉNANFF,
Rapporteurs thématiques

TOME II :
COMPTES RENDUS

Voir les numéros :

Sénat : **33**, **393**, **394** et T.A. **78** (2024-2025).

Assemblée nationale : **1112**.

(1) La composition de cette commission spéciale figure au verso de la présente page.

La commission spéciale est composée de :

M. Philippe Latombe, *président* ;

Mme Virginie Duby-Muller, M. Thomas Gassilloud, M. Laurent Mazaury, M. Hervé Saulignac, *vice-présidents* ;

Mme Amélia Lakrafi, M. Aurélien Lopez-Liguori, Mme Liliana Tanguy, M. Vincent Thiébaut, *secrétaires* ;

M. Éric Bothorel, *rapporteur général* ;

M. Mickaël Bouloux, Mme Catherine Hervieu, Mme Anne Le Hénanff, *rapporteurs thématiques* ;

M. Xavier Albertini, M. Pouria Amirshahi, M. Rodrigo Arenas, Mme Bénédicte Auzanot, Mme Lisa Belluco, M. Édouard Bénard, M. Ugo Bernalicis, M. Matthieu Bloch, Mme Émilie Bonnivard, Mme Manon Bouquin, M. Jérôme Buisson, M. Eddy Casterman, M. François Cormier-Bouligeon, M. Jean-François Coulomme, Mme Geneviève Darrieussecq, M. Hervé de Lépinau, Mme Élisabeth de Maistre, Mme Sandra Delannoy, Mme Sophie Errante, M. Yannick Favennec-Bécot, Mme Marina Ferrari, M. Julien Gabarron, Mme Olga Givernet, M. Philippe Gosselin, M. Patrick Hetzel, M. Sébastien Huyghe, Mme Marietta Karamanli, M. Bastien Lachaud, M. Tristan Lahais, M. Maxime Laisney, Mme Constance Le Grip, M. Denis Masséglia, M. Emmanuel Maurel, M. Paul Midy, M. Jacques Oberti, M. René Pilato, M. Stéphane Rambaud, M. Julien Rancoule, Mme Marie Récalde, M. Matthias Renault, Mme Véronique Riotton, Mme Marie-Ange Rousselot, M. Alexandre Sabatou, M. Arnaud Saint-Martin, M. Sébastien Saint-Pasteur, Mme Laetitia Saint-Paul, M. Aurélien Saintoul, M. Emeric Salmon, M. Philippe Schreck, Mme Sabrina Sebaihi, M. Aurélien Taché, Mme Sabine Thillaye, Mme Mélanie Thomin, M. Roger Vicot, M. Antoine Villedieu, Mme Estelle Youssouffa, *membres*.

SOMMAIRE

___

Pages

COMPTES RENDUS

I. AUDITIONS DE LA COMMISSION SPÉCIALE

1. Première audition de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI), mercredi 7 mai 2025 à 16 heures 30

Lors de sa réunion du mercredi 7 mai 2025, la commission spéciale a auditionné M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et M. Gaëtan Poncelin de Raucourt, sous-directeur « Stratégie ».

M. le président Philippe Latombe. Nous ouvrons aujourd'hui la première réunion plénière de notre commission spéciale par une audition particulièrement structurante.

Nous avons l'honneur d'accueillir M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Avant d'entrer dans le cœur de nos échanges, je souhaite vous informer d'une évolution importante concernant le calendrier d'examen du projet de loi dont notre commission est saisie. L'examen du texte, initialement prévu en séance publique à la mi-juin, a été reporté. À ce jour, aucune date officielle n'a été communiquée. Il est néanmoins possible que l'examen en séance se tienne lors d'une session extraordinaire en juillet ou en septembre. Par conséquent, l'examen du texte en commission spéciale pourrait avoir lieu dès la semaine du 17 ou du 24 juin, si la séance publique se tenait en juillet ou au début de la session extraordinaire de septembre. Dans l'hypothèse d'un examen en séance à partir de la semaine du 15 septembre, nos travaux pourraient se dérouler début septembre, avec un délai de dépôt des amendements à prévoir pour le dernier week-end d'août. Je m'engage à vous tenir informés le plus rapidement possible.

Monsieur le directeur général, l'Anssi, que vous dirigez depuis janvier 2023, après avoir exercé diverses fonctions pendant près de quinze ans et deux ans à la direction de l'opérateur des systèmes d'information interministériels classifiés (Osiic), est aujourd'hui un pilier incontournable de la sécurité des systèmes d'information en France. Service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Anssi veille à la sécurité des systèmes d'information de l'État, accompagne les opérateurs d'importance vitale et participe à la recherche et à la promotion des technologies de sécurité. Votre rôle va s'intensifier dans le cadre du projet de loi que nous examinons, notamment avec l'article 5, qui vous désigne comme le « chef d'orchestre » de la politique gouvernementale en matière de sécurité des systèmes d'information.

Dans son panorama de la cybermenace 2024, publié en mars dernier, l'Anssi dressait un constat préoccupant : 4 386 événements de sécurité traités en 2023, soit une hausse de 15 % par rapport à l'année précédente. Deux types de menaces dominent : la cybercriminalité systémique et les attaques émanant d'acteurs réputés liés à des États, notamment la Russie et la Chine.

Mes collègues et moi-même avons de nombreuses questions à vous poser afin de mieux cerner les enjeux de la transposition de la directive dite NIS 2, ses implications opérationnelles et ses perspectives stratégiques pour la France et l'Europe.

Premièrement, la transposition belge a fait le choix de s'appuyer sur des normes internationales, apportant visibilité et stabilité aux organisations. Ce n'est pas l'option retenue par le projet de loi français, alors que de nombreux acteurs publics et privés y sont favorables, notamment dans une optique d'harmonisation européenne. Pourriez-vous nous éclairer sur ce choix et nous indiquer comment nous pourrions construire une convergence européenne sur le sujet ?

Deuxièmement, le sénateur Olivier Cadic évoquait récemment le risque qu'une sous-transposition législative génère une surtransposition administrative. Pensez-vous que le texte issu du Sénat nécessite des modifications, car il serait trop contraignant ou restrictif ? Comment éviter une inflation de référentiels techniques administratifs, parfois contradictoires, source de confusion pour les acteurs concernés ? Je pense notamment aux retours formulés lors du Forum international de la cybersécurité à propos des sondes issues de la dernière loi de programmation militaire (LPM).

Troisièmement, le règlement général sur la protection des données (RGPD) a prévu la création d'un délégué à la protection des données (DPO), fonction assortie de protections spécifiques. De nombreux auteurs universitaires ont proposé la création d'une fonction de type responsable de la sécurité des systèmes d'information (RSSI), munie de protections adéquates par analogie au DPO. Cette idée est également reprise par des organisations matures en protection cyber, entreprises NIS ou collectivités de grande taille. Pensez-vous que le législateur doit s'emparer de cette proposition et, si oui, doit-il l'imposer ou seulement la suggérer pour une partie des entités soumises à NIS 2 ?

Quatrièmement, comment pouvons-nous, selon vous, profiter de ce texte de transposition pour permettre la création d'une base industrielle et technologique de cybersécurité française et européenne (BITC), par analogie à la base industrielle et technologique de défense (BITD), qui participerait à l'autonomie stratégique française et européenne ?

Cinquièmement, quelle interprétation faites-vous de l'avis du Conseil d'État sur la disparité de traitement entre les entités privées soumises à sanctions et les entités publiques dispensées ? Comment envisager de dispenser des entités publiques, par exemple France Travail, de sanctions en cas de manquement avéré

en matière de cybersécurité ? Plus largement, quelle exemplarité doivent avoir l'État et les entités publiques en la matière ?

Enfin, sixièmement, que pensez-vous de la rédaction de l'article 16 *bis* sur le chiffrement ?

Monsieur le directeur général, je vous cède la parole.

M. Vincent Strubel, directeur général de l'Anssi. Concernant la genèse du texte, je me concentrerai sur le titre II, qui transpose la directive NIS 2, les titres Ier et III transposant la directive sur la résilience des entités critiques (REC) et le Digital Operational Resilience Act (Dora), qui relèvent moins de l'Anssi.

La directive NIS 2 nous a été imposée par l'évolution de la menace. Nous traitons depuis des années une menace étatique d'espionnage et potentiellement de sabotage, mais s'y ajoute, depuis le tournant des années 2020, ce que nous appelons la « menace systémique ». Cette dernière est principalement portée par des acteurs du crime organisé et de l'activisme. Elle se caractérise par son caractère non ciblé, contrairement à la menace étatique, et finit par toucher l'ensemble des acteurs. Les entités les plus vulnérables en termes de cybersécurité, auparavant épargnées, sont désormais concernées : petites et moyennes entreprises (PME), entreprises de taille intermédiaire (ETI), collectivités ou encore associations. Cette tendance, observée depuis 2020, ne fait que se confirmer année après année. Les chiffres de notre panorama de la menace corroborent ce constat.

Face à cette situation, partagée à l'échelle européenne, nous avons collectivement élaboré la directive NIS 2, avec une forte impulsion française. Cette directive complète un paysage normatif européen préexistant, notamment la directive NIS 1, mais s'inscrit dans une logique différente. NIS 2 représente un changement d'échelle dans le nombre d'entités régulées. En France, nous passerons de quelques centaines à environ 15 000 entités régulées, avec des proportions similaires dans les autres pays européens. Ce texte marque également un changement de paradigme dans le niveau d'exigence. Nous n'appliquerons pas le même niveau d'exigence à une entreprise de taille moyenne qu'à un opérateur d'importance vitale. De plus, la logique de désignation par seuil remplace la désignation individuelle et nous introduisons des sanctions administratives et financières.

Ce texte répond à une nécessité essentielle pour la résilience de notre économie et de notre société face à une menace qui n'épargne plus personne. Cette menace, actuellement opportuniste, pourrait un jour s'avérer coordonnée avec des menaces étatiques dans un contexte géopolitique plus large.

Au-delà de cette nécessité, je suis convaincu que ce texte représente une véritable opportunité. Il permet de sensibiliser à grande échelle l'ensemble des petites structures jusqu'ici éloignées des enjeux de cybersécurité, mais qui ne peuvent plus les ignorer. Il offre également la possibilité de définir simplement et clairement les bonnes pratiques de cybersécurité pour ces entités, tout en délimitant

leurs responsabilités. Enfin, il constitue une occasion de mobiliser l'écosystème de cybersécurité national et européen, florissant et riche, qui sera naturellement positionné en proximité pour répondre aux besoins de ces petites structures.

Nous nous sommes efforcés de transposer la genèse de la directive dans le projet qui nous est soumis, en suivant plusieurs grands principes.

Nous appliquons tout d'abord le principe de coconstruction, sans précédent pour l'Anssi. Nous avons consulté près de 80 organisations professionnelles et toutes les associations d'élus. Ces consultations, initiées en septembre 2023, se poursuivent dans la préparation des textes d'application et continueront lors de la mise en œuvre.

Ensuite, un autre principe est l'harmonisation, qui se traduit par l'absence de surtransposition. Nous avons effectué une transposition sèche, sans surtransposition ni sous-transposition. Cette recherche d'harmonisation se poursuit dans nos échanges au sein du groupe de coopération NIS 2, avec la Commission et les autres États membres. Nous cherchons à clarifier certains points de mise en œuvre, notamment l'application aux filiales, sujet qui fait l'objet de nombreux débats partagés par l'ensemble des États membres. Nous avons sollicité un avis consensuel de la Commission pour guider notre interprétation et éviter de créer de la complexité inutile.

Par ailleurs, nous appliquons le principe de proportionnalité, prévu par la directive, qui distingue deux types d'entités : les entités essentielles, plus matures en termes de cybersécurité et plus critiques, et les entités importantes, de taille et de maturité moindres. Nous n'aurons pas le même niveau d'exigence sur ces deux types d'entités. Cette proportionnalité se décline dans le régime de sanctions, différencié selon le type d'entité, et dans le régime de contrôle, *ex ante* pour les entités essentielles et *ex post* pour les entités importantes. Ce principe s'applique également aux niveaux d'exigence technique que nous porterons.

Cette approche nous différencie de celle adoptée par nos homologues belges. Notre diagnostic actuel suggère que leur approche est potentiellement moins exigeante pour les entités essentielles, mais probablement plus contraignante pour les entités importantes. L'utilisation de la norme ISO 27001 par les Belges impose à ces entités un travail d'analyse et d'expertise significatif que nous ne comptons pas exiger des entités importantes, car elles ne disposent pas nécessairement de cette expertise.

En outre, nous appliquons un principe de simplification et de rationalisation, qui nous conduit à aligner les différents cadres normatifs préexistants, tels que celui des opérateurs d'importance vitale et celui applicable aux administrations via le référentiel général de sécurité, sur un socle commun de mesures. Nous le compléterons d'exigences supplémentaires pour des entités spécifiques, notamment les opérateurs d'importance vitale. Concernant les sondes de détection, après dix ans de mise en œuvre du dispositif applicable aux opérateurs d'importance vitale,

nous réexaminerons les dispositions et leur efficacité à l'aune de l'état de l'art du moment.

Le texte a été examiné au Sénat en mars. Je salue le travail des sénateurs, qui a amélioré et clarifié le texte, contribuant à l'effort de pédagogie sur ces enjeux pour sensibiliser les entités qui seront concernées par ce texte. Je ne doute pas que l'Assemblée nationale apportera une contribution similaire, tant sur le texte que sur l'accompagnement et la pédagogie nécessaires.

Parmi les évolutions saillantes apportées par le Sénat, je soulignerai l'inclusion dans la loi de certains éléments en termes de définition, de champ d'application et de délais, qui apportent de la visibilité. Cependant, le bon équilibre a été maintenu en préservant la possibilité pour le pouvoir réglementaire d'apporter certaines précisions, notamment sur la définition des secteurs soumis à la directive NIS 2. Cette flexibilité nous permettra de continuer à adapter le déploiement de ce cadre, notamment en lien avec les travaux que nous poursuivons avec nos homologues européens pour clarifier certaines définitions ou interprétations.

Le Sénat a également introduit la possibilité de créer un label national permettant aux entités d'attester leur conformité à NIS 2. Ce label pourra être valorisé auprès d'autres acteurs, tels que les assureurs, les banques ou les clients pour témoigner d'un niveau de sécurité satisfaisant. Nous pouvons nous réjouir de cette évolution et du bon équilibre trouvé, ce label étant une possibilité, et non une contrainte pour les entités assujetties à NIS 2. Nous aurons peut-être à apporter quelques améliorations, à des fins de sécurité juridique, à cette disposition, mais l'équilibre atteint par le Sénat semble approprié.

J'accueille favorablement la possibilité apportée par le Sénat de créer une reconnaissance de labels délivrés par d'autres États membres. Cette initiative répond notamment à la question de l'articulation avec le dispositif belge, et potentiellement avec d'autres dispositifs équivalents qui pourraient être mis en place par d'autres États membres. L'équilibre trouvé me semble judicieux : il s'agit d'une possibilité, et non d'une automaticité, préservant ainsi une marge d'appréciation quant au niveau d'exigence porté par d'autres labels équivalents. Nous aurons également quelques éléments à proposer en termes de sécurisation juridique de ce dispositif.

Certains points soulèvent des interrogations.

Le Sénat a simplifié l'articulation entre Dora et la directive NIS 2, ce qui est louable dans l'intention. Toutefois, supprimer la notification des incidents cyber qui affecteraient les entités soumises à Dora auprès de l'Anssi, pour ne conserver qu'une notification aux entités de contrôle Dora — à savoir l'autorité de contrôle prudentiel et de résolution (ACPR) et l'autorité des marchés financiers (AMF) —, provoque des effets de bord néfastes. Contrairement à l'Anssi, l'ACPR et l'AMF ne disposent pas d'un service opérationnel 24 heures sur 24 et 7 jours sur 7. Ce passage obligé par les autorités de Dora entraînerait un retard dans la prise en

compte des notifications d'incidents par l'Anssi, l'empêchant ainsi de remplir efficacement sa mission d'assistance aux victimes et d'alerte des autres cibles potentielles. Nous proposerons donc de rétablir une forme de double notification, basée sur un formulaire unique pour éviter la duplication du travail, afin de garantir l'efficacité dans le traitement des incidents.

De même, nous nous interrogeons sur les restrictions apportées à la commission des sanctions, indépendante de l'Anssi, mais chargée d'examiner et de prononcer d'éventuelles sanctions à la suite de manquements. Certaines contraintes apportées à sa composition et à ses modalités d'instruction soulèvent potentiellement des risques pratiques quant à sa capacité à disposer de l'expertise nécessaire et à la solidité juridique de ses décisions. Nous sommes à votre disposition pour travailler sur ces enjeux, ainsi que sur des clarifications concernant la responsabilité des organes de direction des entités assujetties.

Parallèlement au processus législatif, nous avons initié des travaux préparatoires pour répondre à deux besoins majeurs exprimés lors de nos consultations : une mise en œuvre progressive et un accompagnement adapté.

Concernant la mise en œuvre progressive, je réaffirme notre souhait de prendre le temps nécessaire à une mise en œuvre adéquate de ces dispositions en distinguant les obligations simples, telles que l'enregistrement auprès de l'Anssi et la notification d'incidents – qui bénéficieront d'un délai de six mois –, des obligations plus complexes pour lesquelles nous accorderons un délai de trois ans après la publication des textes d'application, avec une approche progressive incluant des contrôles à blanc sans sanction durant cette période.

Concernant l'accompagnement, nous travaillerons sur trois axes.

Premièrement, nous développons une offre de services adaptée et clarifiée de la part de l'Anssi, comprenant des dispositifs tels que « Mon Aide Cyber » pour un premier diagnostic, « Mes Services Cyber » pour une meilleure lisibilité du corpus documentaire et « Mon Espace NIS 2 » pour le préenregistrement et le test de la soumission au cadre NIS 2.

Deuxièmement, nous mettons en place un réseau de relais impliquant les services de l'État, les collectivités, les organisations professionnelles et l'écosystème des fournisseurs de produits et services français et européens. La logique de cet accompagnement vise à n'exclure personne et à partager un cadre commun ainsi qu'une offre lisible.

Troisièmement, nous mobilisons tous les dispositifs de soutien et d'accompagnement, publics et privés, y compris à travers la perspective d'un label facilitant la démonstration de conformité et l'appréciation des risques par les secteurs bancaire et assurantiel.

Enfin, un enjeu transverse est celui de la communication. Il est impératif de sensibiliser toutes les futures entités assujetties, qui sont souvent éloignées des

préoccupations de cybersécurité et qui ont besoin de s'en préoccuper avant de subir des attaques. Je ne doute pas que vos travaux contribueront à cette sensibilisation. L'Anssi se tient à votre disposition pour vous y aider.

M. le président Philippe Latombe. Je cède la parole aux rapporteurs.

M. Éric Bothorel, rapporteur général. Je me permets de suggérer que nous puissions auditionner une nouvelle fois M. le directeur général à l'issue de nos travaux. En effet, il me semble aussi pertinent de l'auditionner aujourd'hui, en introduction de nos travaux, qu'après avoir entendu un certain nombre d'acteurs qui ne manqueront pas de nous faire part de leurs observations et recommandations.

Concernant le calendrier que vous avez évoqué, monsieur le président, je souhaiterais que nous puissions mener nos travaux de manière continue. C'est un avis personnel, mais s'il était partagé par d'autres, peut-être pourrait-il être pris en considération.

Dans mon mandat de rapporteur général, je serai attentif à rechercher les équilibres concernant un texte qui se veut harmonieux, de par sa nature européenne. Lorsqu'on est attaché à une forme de souveraineté, qui ne doit pas être confondue avec du souverainisme, il est en effet impératif de disposer d'un cadre européen harmonieux plutôt que fragmenté. En tant que rapporteur général, je veillerai à ce que ces équilibres soient respectés.

Monsieur le directeur général, nous entendons parfois qu'il est inutile de s'embarrasser avec ces actions, puisque la norme ISO 27001 est excellente et permet de se passer de nuances technologiques et de spécificités techniques rappelées dans ces trois textes.

Par ailleurs, au-delà de l'articulation de Dora et de NIS 2, comment parvenez-vous à trouver un équilibre avec les autres organisations, notamment la Commission nationale de l'informatique et des libertés (Cnil) ?

Comment pouvons-nous faire en sorte que NIS 2 devienne un sujet de levier et de démultiplication de notre écosystème cyber ?

Enfin, concernant le chiffrement, pourriez-vous apporter une réponse plus précise à la question du président ?

Mme Anne Le Hénanff, rapporteure. Les sénateurs ont directement inscrit dans la loi la liste des secteurs, en distinguant ceux considérés comme hautement critiques de ceux critiques. Un décret en Conseil d'État précisera les sous-secteurs et les types d'entités relevant de ces deux catégories. Quelle est votre opinion sur cette approche des sénateurs ?

Concernant le budget nécessaire pour se mettre en conformité, comment envisagez-vous l'accompagnement des territoires des entités concernées et la mise en œuvre de la directive par ces mêmes entités ? Avez-vous déjà évoqué la question

des moyens financiers ou cela reste-t-il à définir dans le cadre d'un projet de loi de finances (PLF) ?

La sénatrice Vanina Paoli-Gagin a évoqué les critères de sélection des contrôleurs, en insistant sur la nécessité qu'ils soient français pour éviter les risques d'ingérence. Pouvez-vous nous en dire davantage à ce sujet ? Pourquoi avez-vous exprimé un avis défavorable au Sénat sur ce point ?

Enfin, pourriez-vous nous éclairer sur le niveau de protection des mesures mises en place dans la transposition de NIS 2, comparativement aux exigences actuelles en vigueur appliquées aux opérateurs d'importance vitale, notamment dans le cadre de la LPM 2013 ?

M. Mickaël Bouloux, rapporteur. En tant que rapporteur thématique sur le titre III du projet de loi, qui est relatif à la résilience opérationnelle numérique du secteur financier et qui ne concerne pas autant l'Anssi que la transposition de la directive NIS 2, je souhaite vous poser quelques questions sur le rôle de votre agence dans la résilience des entités financières.

Tout d'abord, pourriez-vous nous donner des exemples récents de cybermenaces auxquelles sont exposés les acteurs du système financier ? La recapitalisation de la filiale américaine de la banque chinoise ICBC est souvent citée comme exemple. J'ai lu, dans votre dernier panorama, que le logiciel financier Xtrader avait aussi été compromis.

Ensuite, compte tenu des menaces, pensez-vous que le règlement et la directive Dora seront décisifs pour assurer la résilience du secteur financier ?

Enfin, le Sénat a ajouté deux articles additionnels au titre III du projet de loi afin de désigner une seule autorité compétente pour recevoir, de la part des entités financières, les déclarations obligatoires d'incidents majeurs et les notifications volontaires de cybermenaces importantes pour respecter l'article 19 du règlement Dora. Si cet ajout est motivé par le souhait d'éviter le double assujettissement entre NIS 2 et Dora, vous militez pour que l'Anssi puisse également être prévenue. En tant que rapporteur thématique, je suis enclin à soutenir ce point.

Mme Catherine Hervieu, rapporteure. Je suis rapporteure pour le titre I^{er}, relatif à la résilience des activités d'importance vitale pour l'ensemble des thématiques que nous aborderons à travers ce sujet.

La cybersécurité de l'État doit être renforcée pour protéger nos données et nos secteurs critiques. L'objectif stratégique n° 4 de la revue nationale stratégique (RNS) 2022, visant une résilience cyber de premier rang, est plus que jamais d'actualité. Il est impératif de rehausser le niveau de cybersécurité de l'ensemble des entités importantes, face à des besoins qui s'accélèrent quotidiennement. La mise en place d'une stratégie nationale en matière de cybersécurité est donc primordiale, notamment pour une question de défense nationale.

La directive NIS 2 représente une avancée significative pour assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne. Elle participe à une transformation de l'Anssi, modifiant vos méthodes de travail et vos échanges avec vos interlocuteurs. Votre rôle est central pour informer et accompagner des acteurs de notre territoire en matière de cybersécurité des entités importantes.

Quelles sont les conséquences du texte sur les collectivités territoriales, dont les moyens sont très hétéroclites, tant sur le plan humain que financier ? Comment envisagez-vous de déployer l'accompagnement en tenant compte des contextes territoriaux ?

La coopération stratégique et l'échange d'informations entre les États membres, ainsi que le réseau des *Cyber Incident Response Teams* (CIRT) qui favorise une coopération opérationnelle rapide et efficace entre les entités nationales, sont des moyens d'améliorer la cybersécurité à tous les échelons. Pourriez-vous développer vos besoins en matière de coopération avec les États membres de l'Union européenne ?

Enfin, face aux évolutions technologiques exponentielles, notamment l'intelligence artificielle, comment appréhendez-vous notre prise en compte de ces enjeux, en particulier pour les technologies de rupture ?

M. Vincent Strubel, directeur général de l'Anssi. Concernant les exigences ISO 27001, nous n'y sommes pas opposés. La plupart de nos référentiels de prestataires qualifiés déclinent la même architecture que cette norme. Cependant, elle ne constitue pas l'outil adéquat pour répondre aux exigences de NIS 2. Nos homologues belges partagent cette analyse : ils se sont certes inspirés de la norme ISO 27001, mais l'ont complétée par des exigences supplémentaires. Par exemple, ISO 27001 ne traite pas la question des sauvegardes, pourtant cruciale pour les petites entreprises face aux rançongiciels. Nous intégrerons ce type d'exigences, à l'instar des Belges. Nous ne nous contentons donc pas d'une simple déclinaison d'une norme sur étagère.

Une autre réserve concernant l'ISO 27001 tient à sa nature : il s'agit d'une méthode pour élaborer des objectifs de sécurité et se mettre en conformité. Cette norme n'indique pas précisément les actions à entreprendre pour répondre à un niveau de menace précis. Ce travail d'adaptation incombe à l'entité appliquant la norme. Nous estimons donc que cette démarche sera trop complexe pour de petites structures, notamment parmi les entités importantes qui ne disposeront pas toutes d'un RSSI.

Bien que le métier de RSSI soit indispensable, je ne suis pas convaincu de la nécessité de l'encadrer par la loi. De nombreux RSSI exercent aujourd'hui sans ancrage légal et ils ne semblent pas en avoir besoin. En revanche, nous n'envisageons pas d'exiger la présence d'un RSSI ou d'un expert en cybersécurité dans chaque entité importante, ce qui serait déraisonnable au vu de la taille de

certaines d'entre elles. Nous procéderons plutôt à une analyse des risques au profit des secteurs d'activité et proposerons des mesures relativement simples à mettre en œuvre.

Concernant le positionnement entre NIS 2 et le cadre applicable aux opérateurs d'importance vitale, nos exigences seront nettement moins strictes pour NIS 2 que pour les opérateurs d'importance vitale. Néanmoins, cela constituera le socle commun. Pour les opérateurs d'importance vitale, dans le cadre de la refonte du dispositif d'activité d'importance vitale portée par le titre Ier, nous ajouterons des mesures complémentaires reprenant certaines exigences spécifiques actuellement en vigueur. Ces exigences sont pertinentes compte tenu de leur niveau d'exposition à la menace, y compris stratégique. Les opérateurs d'importance vitale sont concernés non seulement par la menace systémique, mais aussi par des menaces ciblées. Nous maintiendrons donc des exigences en matière de détection, qui figure dans le cadre existant, mais que nous actualiserons au gré de l'évolution de l'état de l'art, tandis que nous appliquerons un niveau d'exigence moindre pour les entités soumises à NIS 2, en raison de leur exposition différente à la menace et de leurs moyens plus limités.

Quant à l'intelligence artificielle, notre analyse, largement partagée lors du sommet pour l'action sur l'intelligence artificielle, ne la considère pas comme une rupture fondamentale en matière de cybersécurité. Elle améliorera certes les capacités des attaquants, mais aussi celles des défenseurs. Il s'agit, pour nous, de nous emparer de ces nouvelles technologies au même rythme que les « méchants » et d'accompagner le déploiement de l'intelligence artificielle par des mesures de cybersécurité appropriées. Toutefois, le rapport d'analyse des risques que nous avons publié, cosigné par deux de nos partenaires étrangers, souligne que le déploiement de l'intelligence artificielle nécessite avant tout le respect des bonnes pratiques de base applicables à tout logiciel, avant de se préoccuper d'autres risques spécifiques. Le socle de base de bonnes pratiques que nous porterons avec NIS 2 devrait largement résister à l'épreuve du temps et permettre une prise en compte adéquate de ces enjeux, tout en restant ouvert à d'éventuelles révisions.

La nécessité d'une bonne articulation entre les niveaux législatif et réglementaire découle du besoin d'ajuster les mesures en fonction de l'évolution technologique.

Concernant la liste des secteurs inclus dans la loi par le Sénat, elle reprend littéralement ceux prévus par la directive. Initialement, nous avions jugé cette reprise superflue, mais nous respectons la décision du Sénat, qui estime que cela contribue à la lisibilité du texte. Nous ne sommes pas opposés à cette décision tant que nous conservons la possibilité de préciser les sous-secteurs au niveau réglementaire, notamment pour permettre l'articulation avec les définitions retenues dans les périmètres ministériels, susceptibles d'évoluer. Le point d'équilibre trouvé par le Sénat nous semble satisfaisant à ce stade.

Concernant l'articulation avec les entités des cadres Dora et RGPD, parmi lesquels la Cnil, nous suivons le principe de *lex specialis* prévu par les directives. Les entités soumises à Dora et à NIS 2 appliquent les règles de Dora, et non les règles équivalentes de NIS 2. Elles appliquent en outre les règles de NIS 2 lorsqu'il n'en existe pas d'équivalentes dans Dora. Concrètement, elles appliqueront toutes les règles Dora, plus deux règles supplémentaires présentes dans NIS 2 : l'enregistrement auprès de l'Anssi et la notification des incidents de cybersécurité à cette même autorité.

Le Sénat a simplifié la deuxième exigence en prévoyant le principe de simple notification. Si l'intention est louable, l'effet me semble potentiellement problématique. Nous pensons qu'un formulaire commun envoyé aux deux entités de contrôle serait préférable. Nous avons évidemment entamé des discussions avec les autorités de contrôle Dora, à savoir l'ACPR et l'AMF, pour partager notre compréhension des exigences et coordonner nos contrôles. Un principe similaire s'appliquera *a priori* pour l'articulation avec le cadre RGPD, en concertation avec la Cnil.

Le projet de loi établit un principe de *non bis in idem*. Lorsqu'une sanction est envisagée au titre de NIS 2 et du RGPD, le régime de sanctions pécuniaires appliqué sera celui du RGPD, considéré comme plus disant en termes de pourcentage du chiffre d'affaires global.

Nous menons actuellement une concertation avec la Cnil concernant les modalités de contrôle, le partage des retours d'expérience, l'interprétation des exigences et le traitement des incidents. Le projet de loi prévoit un équilibre judicieux : nous avons la possibilité de notifier à la Cnil des manquements évidents à la protection des données personnelles, mais ce n'est pas le principe par défaut. Nous privilégions plutôt l'approche qui est déjà la nôtre dans le traitement des incidents. Quand nous assistons une victime de cyberattaques, nous l'invitons à se préoccuper des enjeux de données personnelles, lui expliquons le cadre applicable et la mettons en relation, le cas échéant, avec la Cnil et lui donnons accès à tous les formulaires applicables, mais nous ne réalisons pas, à sa place, le travail d'estimation des impacts sur les données personnelles. Cet équilibre se dessine et semble faire consensus avec la Cnil.

Concernant les critères de sélection des contrôleurs, le gouvernement a défendu au Sénat la proposition que, pour NIS 2, le contrôle sera effectué par l'Anssi, avec la possibilité de s'appuyer sur des tiers, y compris des agents de l'ACPR ou de la Cnil, et de faire appel à des acteurs du secteur privé. Il n'est pas nécessaire de rigidifier ce cadre dans la loi.

Par ailleurs, concernant l'articulation avec les collectivités territoriales, le gouvernement a choisi de ne pas imposer de sanctions financières, estimant que priver les collectivités de ressources ne favoriserait pas le développement de leur maturité en matière de cybersécurité. En revanche, d'autres mesures, telles que la publicité des manquements, sont considérées comme des moyens efficaces pour

rappeler à l'ordre les collectivités qui ne joueraient pas le jeu. Ce choix du gouvernement est laissé à votre appréciation.

La déclinaison du dispositif pour les collectivités suit une approche comparable à celle d'autres États membres : les régions, départements et grandes agglomérations sont classés comme entités essentielles, les intercommunalités plus petites comme entités importantes, tandis que les communes individuelles ne sont pas directement concernées.

Je ne m'aventurerai pas sur le sujet des moyens budgétaires des collectivités, n'étant pas forcément légitime à porter la position du gouvernement sur ce point. Nous mobiliserons évidemment toutes les possibilités d'accompagnement, ce que nous faisons déjà. Nous avons soutenu, à travers le plan de relance, l'accompagnement méthodologique et l'incubation, ainsi que le développement des CIRT régionaux, complémentaires de l'action de l'Anssi. Il est prévu, dans le cadre de la transposition, que nous travaillerons avec ces CIRT, bien que je n'ai pas moi-même de réponse à la question de leur financement.

Sur le volet industriel, ma conviction est que cette directive représente une opportunité pour tout le tissu industriel, en particulier de proximité. Nous mobiliserons les experts cyber et les prestataires pour les accompagner dans cette transition. Je ne crois pas que cela se fasse en priorité au bénéfice d'acteurs non européens, qui ne sont pas nécessairement positionnés sur ce segment. Par conséquent, je ne juge pas nécessaire d'imposer le recours à des prestataires français.

Enfin, concernant le chiffrement, je comprends la teneur politique de l'article 16 *bis*. L'Anssi est évidemment très attachée, par nature, à la défense d'un chiffrement robuste, l'une de nos premières armes de protection contre les cybermenaces. De ce point de vue, l'article 16 *bis* affirme des principes que nous soutenons. Toutefois, sur le plan juridique, je ne sais pas s'il est nécessaire de le dire dans la loi. Je ne me prononcerai pas sur une éventuelle modification de cet article. Je dirai simplement que la protection du chiffrement et le pouvoir d'enquête des services judiciaires méritent un examen approfondi et ne peuvent être traités trop rapidement. Un travail au niveau technique est donc nécessaire sur ces sujets, avant de revenir au législateur, le cas échéant, afin qu'il arbitre. Ma conviction personnelle est que ce n'est pas dans le cadre du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité que nous résoudrons le problème fondamental porté devant le législateur dans le cadre de l'examen de la proposition de loi visant à sortir la France du piège du narcotrafic.

M. le président Philippe Latombe. Je cède maintenant la parole aux orateurs des groupes parlementaires.

M. Aurélien Lopez-Liguori (RN). Ce texte entraînera notre pays dans un monumental effort de cybersécurité, impliquant plus de 14 500 acteurs, dont des opérateurs d'importance vitale, des hôpitaux, des collectivités et des entreprises. Cet

effort s'inscrit dans un contexte de tensions internationales majeures, où les attaques cyber se multiplient, les États deviennent plus offensifs et l'espionnage se généralise via des règles extraterritoriales qui pullulent. Le numérique est désormais un champ de confrontation directe.

Dans ce contexte, l'effort national demandé doit non seulement servir notre souveraineté, mais aussi stimuler le développement économique de notre filière cyber. La France dispose en effet d'une industrie cyber d'excellence, avec des entreprises innovantes enracinées sur notre territoire, comme Tehtris, Gatewatcher, Ziwit, Wallix et HarfangLab. Ces sociétés ont démontré leur solidité technologique, obtenu des qualifications exigeantes de l'Anssi et contribuent déjà à la protection de nos systèmes vitaux.

Ce texte doit permettre que, pour leur protection cyber, les acteurs cyber concernées se tournent en premier lieu vers des acteurs nationaux et européens. C'est notre rôle, en tant que députés de la nation française, de veiller à ce que les retombées économiques et les externalités positives profitent prioritairement à notre écosystème, plutôt qu'à des sociétés étrangères susceptibles de nous espionner et de menacer nos intérêts via des règles extraterritoriales.

Quelles mesures proposez-vous pour que le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité devienne un levier concret de soutien à notre filière cyber nationale ?

Comment comptez-vous faire en sorte que NIS 2 confère une certaine immunité face aux règles extraterritoriales, à l'espionnage et aux ingérences étrangères ?

Envisagez-vous, dans les textes d'application, la création de labels de certification ou de critères de souveraineté permettant de favoriser les prestataires européens et français plutôt que les acteurs étrangers ?

M. Thomas Gassilloud (EPR). Je tiens à souligner la pertinence de ce texte face aux menaces opportunistes, mais également aux menaces plus structurées pouvant survenir d'États tiers, potentiellement en complément d'autres formes de menaces, y compris de nature cinétique. Je considère ce texte comme une opportunité de consolider notre défense face aux menaces hybrides au sens large, en complément de la démarche nationale entreprise, notamment dans le cadre de la stratégie de résilience.

Quelle articulation est prévue dans ce texte avec le commandement de la cyberdéfense (COMCYBER) ? Comment fonctionnent les interfaces et comment seront traitées les infrastructures critiques duales ?

Concernant la déclinaison territoriale, ce texte offre l'occasion de faire collaborer à froid des acteurs qui ne se connaissent pas nécessairement, autour des services déconcentrés de l'État, des chambres consulaires ou encore des services de l'éducation nationale. Il est crucial de ne pas oublier la chaîne de l'organisation

territoriale interarmées de défense (OTIAD) autour des officiers généraux de zone de défense et des délégués militaires départementaux. J'espère que cette démarche permettra aux acteurs de mieux se connaître pour développer des réflexes utiles en temps de crise.

Enfin, je note que le renseignement d'origine sources ouvertes (Osint) n'est pas spécifiquement mentionné dans le texte, bien qu'il s'agisse d'un outil incontournable en matière de cybersécurité, ne serait-ce que pour identifier une exposition dans une base de données piratée. L'État utilise lui-même l'Osint pour ses services de renseignement et ses questions de sécurité fiscale. Je note que le droit français semble imprécis sur ce point, ce qui incite parfois les acteurs à recourir à des opérateurs étrangers. Pensez-vous qu'il serait nécessaire de renforcer le texte sur cet aspect ?

M. René Pilato (LFI-NFP). Ce projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité place l'Anssi au cœur d'un objectif de résilience, d'où l'importance de cette première audition.

À l'heure où les intelligences artificielles suscitent de nombreuses interrogations et craintes, notamment en raison de leur potentiel de nuisance démultiplié, comment envisagez-vous l'évolution de vos missions face à la multiplication et au changement de nature des attaques liées aux intelligences artificielles, notamment concernant la falsification des données ?

Dans le cadre de votre mission première de protection de la nation, votre agence dispose d'une liste d'organismes d'importance vitale auxquels vous apportez prioritairement votre expertise et vos recommandations en cas de cyberattaque. Pouvez-vous nous indiquer à combien d'entités touchées par semaine ou par mois vous apportez votre expertise et votre soutien face aux attaques suivies ?

Ce projet de loi élabore des listes remaniées, plus larges, en fonction de secteurs hautement critiques pour le fonctionnement de l'économie et de la société, par l'intermédiaire des articles 7 à 10. Pensez-vous disposer des capacités humaines nécessaires pour assurer ces recommandations et protéger efficacement la souveraineté de la nation avec ces nouveaux périmètres ?

Enfin, l'agence que vous représentez est placée au service du premier ministre. Bien que la stratégie nationale en matière de cybersécurité soit une décision politique, je m'étonne de cette mise sous tutelle, alors que c'est votre indépendance qui devrait être notre garantie.

M. Sébastien Saint-Pasteur (SOC). L'Anssi doit être le phare éclairant le chemin de nos travaux, et plus encore celui des très nombreuses nouvelles entités assujetties à cette transposition. Dans le monde réel, la directive NIS 2 est déjà présente sur nos moteurs de recherche, avec des prestataires proposant services et audits moyennant de substantielles rémunérations. L'effet d'aubaine est réel, mais, malheureusement, ces prestations, dont les coûts annuels se chiffrent souvent à cinq chiffres, ne correspondent fréquemment ni aux besoins ni aux attentes dans de

nombreuses situations. Il existe un risque de prestations inadaptées, avec des contrats signés dans l'urgence et dans une certaine méconnaissance, ce qui pourrait engendrer une défiance vis-à-vis de cette régulation pourtant nécessaire. La question d'une labellisation des structures, comme dans le domaine militaire, ou d'un référentiel d'exigences en termes de qualification se pose évidemment.

Il est nécessaire de consolider et renforcer les écosystèmes locaux, notamment les cyber campus, ces centres de réponse aux incidents cyber implantés dans de nombreux territoires. J'ai l'honneur d'avoir le siège du cyber campus Nouvelle-Aquitaine dans ma circonscription et vous connaissez probablement le travail remarquable réalisé en leur sein. Ne pensez-vous pas qu'il soit opportun de renforcer leurs moyens d'action et opérationnels ? Il faut certes des « pompiers » intervenant en cas d'urgence, mais aussi une médecine préventive. Les entreprises et collectivités concernées ont besoin, dans le cadre de cette nouvelle donne que constitue NIS 2, de savoir comment prioriser entre l'accompagnement des utilisateurs, la sensibilisation des directions et des élus dans une collectivité, la sécurité des terminaux ou encore la refonte des systèmes réseaux dans une entreprise.

Ces deux questions visent à éclairer le dernier kilomètre de nos politiques publiques, au plus près des besoins, là où la menace est malheureusement grandissante.

Mme Sabine Thillaye (Dem). Si vous disposez aujourd'hui des ressources humaines et techniques nécessaires à l'exercice de vos missions, il me semble que l'Anssi compte 600 collaborateurs. Des recrutements seraient nécessaires dans votre agence, ainsi que dans les entités dont nous parlons. Or, nous sommes confrontés à un problème de recrutement et de concurrence entre le secteur civil et militaire pour les cyberspécialistes. Comment envisagez-vous de surmonter ce manque de ressources humaines ?

Par ailleurs, l'article 11 de la directive REC prévoit l'obligation, pour les États membres, d'organiser une coopération transfrontalière, notamment via les consultations. Or, contrairement à la directive, le projet de loi ne contient aucune disposition explicite transposant cette obligation. Cette lacune ne risque-t-elle pas de limiter l'efficacité collective de la réponse européenne en matière de protection des infrastructures ?

Enfin, concernant la mise en place du label attestant de la conformité des entités aux exigences de la directive NIS 2, ne craignez-vous pas que le développement de labels nationaux, en l'absence d'une harmonisation européenne, entraîne une fragmentation du marché et des coûts supplémentaires pour les acteurs opérant dans plusieurs États membres ?

M. Vincent Strubel. La coopération transfrontalière est déjà une réalité efficace et extrêmement active. Au niveau technique, elle s'opère via le CSIRTs Network, où la France est représentée par l'Anssi. Sur le plan stratégique, le réseau

CyCLONe, regroupant les directeurs d'agences nationales de cybersécurité, joue un rôle crucial. Notre collaboration s'est notamment illustrée lors de la préparation des Jeux olympiques et paralympiques. Il n'est pas nécessaire d'introduire de nouvelles dispositions législatives pour organiser cette coopération. Le projet de loi comporte déjà quelques éléments visant à faciliter et sécuriser juridiquement l'échange d'informations avec la Commission européenne et nos homologues européens, dans le traitement de crises transfrontalières. Nous croyons profondément à cette coopération, qui est déjà une réalité essentielle, car nous sommes conscients que les incidents cyber ne s'arrêtent pas aux frontières. C'est une réalité quotidienne qui ne nécessite pas d'ajout supplémentaire dans la loi.

Je rejoins les observations faites sur l'effort considérable nécessaire pour développer notre résilience. Cet objectif s'inscrit dans l'objectif stratégique de la RNS et, plus généralement, dans un enjeu de souveraineté. Il s'agit de ne pas être une victime facile face aux cyberattaques, qui constituent une pression quotidienne et peuvent être mobilisées de manière plus coordonnée par certains États, où des acteurs étatiques, cybercriminels et activistes coexistent sans être inquiétés par les autorités répressives. Le risque d'une mobilisation massive de ces acteurs pour saboter des pans entiers de notre société et de notre économie est bien réel. Face à cette menace, renforcer notre niveau de résilience devient un défi de souveraineté essentiel. Il s'agit de protéger nos intérêts fondamentaux, d'éviter que des secteurs entiers ne soient facilement compromis et de développer une résilience, même face à des attaques très ciblées.

Bien que la directive NIS 2 ne vise pas principalement à contrer des groupes comme APT28, récemment attribué formellement par la France au renseignement militaire russe, il est crucial de comprendre que même de petites entités peuvent être des victimes indirectes ou des cibles permettant d'accéder à de plus grands groupes. Élever globalement le niveau de résilience, tout en maintenant des exigences raisonnables par rapport à la maturité des acteurs, est un enjeu de sécurité nationale et de souveraineté. C'est essentiel pour nous préparer à un contexte géopolitique qui ne va pas en s'adoucissant.

Concernant le soutien à la filière française et européenne, je ne crois pas à de mesures contraignantes imposant le recours à des prestataires nationaux ou européens. Ce n'est d'ailleurs pas la base légale que donne la directive. Je crois plutôt à la mobilisation de l'écosystème, qui existe déjà, et au travail que nous menons avec les acteurs bénéficiant de visas de sécurité et de la qualification de l'Anssi. Nous avons travaillé sur nos référentiels de prestataires pour inclure des niveaux d'ambition moindres, afin de prévoir des prestations répondant plutôt aux besoins des ETI ou PME. Nous travaillons également avec des réseaux de prestataires proches de l'Anssi, comme les experts cyber labellisés par le groupement d'intérêt public (GIP) Cybermalveillance.gouv.fr. Notre philosophie est de n'exclure personne et de travailler en proximité avec les acteurs nationaux déjà mobilisés sur ce sujet. Nous veillons à prévenir les effets d'aubaine et la vente de prestations mensongères. Il est important de poser rapidement un cadre clair,

applicable et déclinable par tous, même si nous travaillons déjà avec les acteurs de l'écosystème sur ces questions.

Par ailleurs, l'immunité face aux droits extraterritoriaux est évidemment une préoccupation qui se décline dans le référentiel SecNumCloud de l'Anssi, dans la stratégie cloud de l'État, et plus récemment dans la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. Cependant, ce n'est pas le cœur du sujet pour les petites entités concernées par la directive NIS 2. Cette problématique concerne davantage les entreprises stratégiques ou certains secteurs d'activités spécifiques.

En termes d'articulation, nous proposons en revanche de valoriser les prestations disposant d'un visa de sécurité de l'Anssi. Sans l'imposer, nous souhaitons que le recours à un acteur bénéficiant d'un visa de sécurité, d'une recommandation de l'Anssi ou d'un label de confiance apporte une plus-value dans la satisfaction des exigences de la directive NIS 2.

Par ailleurs, en 2024, nous avons traité plus de 4 000 incidents de cybersécurité, concernant non seulement des opérateurs d'importance vitale, mais aussi d'autres entités qui nous sollicitent volontairement.

Il est évident que nous devrons renforcer nos moyens, ce qui fera l'objet de discussions budgétaires ultérieures.

Notre présence territoriale est assurée par un délégué de l'Anssi dans chaque région, coordonnant les acteurs locaux et appliquant notre cadre commun afin d'armer la fonction de contrôle. Nous avons besoin de mobiliser tous les acteurs de proximité, mais je pense qu'un certain nombre d'eux l'est déjà. En outre, la gendarmerie joue un rôle essentiel dans les territoires en utilisant le même outillage que nous, notamment « Mon Aide Cyber », pour établir de premiers diagnostics.

Les campus cyber sont principalement positionnés aux points de rencontre entre des offreurs et des bénéficiaires. Je recommande la prudence quant à l'attribution de missions supplémentaires et je ne juge pas nécessaire de figer leurs missions dans la loi. Chaque campus régional s'inscrit dans un écosystème particulier à l'échelle locale. N'allons pas imposer un modèle unique alors que ce qui existe fonctionne déjà très bien.

Par ailleurs, notre articulation avec le COMCYBER est une réalité quotidienne, notamment au sein du centre de coordination des crises cyber (C4), et nous permet de partager des éléments d'analyse, de compréhension de la menace et d'attribution d'une cyberattaque. Cette coopération nous a récemment permis d'attribuer formellement une cyberattaque marquante à un acteur russe particulièrement présent. Pour les menaces touchant la sphère de la défense, nous travaillons étroitement avec le COMCYBER – qui est autonome sur la sécurité du ministère des armées, mais n'est pas forcément chargé de la sécurité de la BITD – et la direction du renseignement et de la sécurité de la défense (DRSD), sans qu'il soit nécessaire de formaliser davantage cette collaboration dans la loi.

La déclinaison territoriale des bons réflexes de sécurité est un enjeu fondamental, qui ne sera pas seulement porté par la loi. Nous croyons beaucoup aux vertus des entraînements et des exercices, comme nous l'avons fait pour la préparation des Jeux olympiques et paralympiques ou la sécurisation des hôpitaux. À une échelle encore plus grande, dans la perspective du déploiement de NIS 2, nous organiserons l'exercice massif REMPAR25 en octobre 2025, qui mobilisera des collectivités et visera à entraîner les décideurs à la gestion de crises cyber.

Enfin, l'Osint fait partie de la panoplie de la réponse ou de l'anticipation des attaques. L'Anssi pratique Osint comme tout acteur de cybersécurité. Si je suis favorable à l'utilisation de l'Osint, je ne suis néanmoins pas certain qu'une base légale soit nécessaire, car son utilisation ne semble pas illégale dans son état actuel. Je suis ouvert à d'éventuelles propositions d'ajustement, mais, si rien n'empêche le recours à des prestations d'Osint, il ne semble pas nécessaire d'imposer un cadre légal.

M. le président Philippe Latombe. Je cède la parole aux députés pour leurs questions individuelles.

M. Emeric Salmon (RN). Depuis 2013, la loi impose aux opérateurs d'importance vitale d'utiliser des solutions qualifiées par l'Anssi et opérées depuis la France, garantissant ainsi fiabilité et souveraineté. L'article 16 du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité revient sur ce principe. Les opérateurs d'importance vitale utiliseront des produits certifiés, agréés ou qualifiés, la seule qualification, plus exigeante, n'étant plus obligatoire. Le label actuel serait supprimé et remplacé par les exigences issues de cette loi. Pire encore, l'article supprime toute obligation légale de localisation en France pour ces solutions. Cette mesure représente un recul significatif, affaiblissant la protection de nos données les plus sensibles et pénalisant les entreprises françaises ayant investi pour répondre à ces standards.

Pourquoi abandonner un dispositif éprouvé depuis dix ans ?

Les nouvelles règles offriront-elles au moins le même niveau de protection ?

Envisagez-vous d'intégrer un critère de souveraineté pour les prestataires chargés de protéger nos infrastructures vitales ?

M. Vincent Strubel. Je n'ai pas la même lecture de la loi. Le cadre cyber qui s'impose aux opérateurs d'importance vitale est porté par le code de la défense, rénové à travers la transposition de la directive REC. Notre objectif est d'inscrire dans la loi des exigences similaires. Les articles concernés du code de la défense sont relativement succincts et se déclinent ensuite au niveau réglementaire par le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité des systèmes d'information et le décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première

partie de la partie législative du code de la défense, ainsi que par des arrêtés sectoriels définissant des exigences spécifiques. La LPM de 2013 et l'article que cette dernière introduit dans le code de la défense nous permettent d'imposer, dans certains cas, le recours à des solutions qualifiées pour les opérateurs d'importance vitale. La proposition actuelle suit la même logique, en établissant une base légale qui sera ensuite déclinée au niveau réglementaire.

Actuellement, trois obligations s'imposent spécifiquement aux opérateurs d'importance vitale : le recours à des prestataires d'audit de sécurité des systèmes d'information (PASSI), qualifiés par l'Anssi, ainsi que le recours à des prestataires de détection et à des sondes réseaux de détection, également qualifiés par l'Anssi.

L'esprit du travail d'actualisation, en lien avec le titre Ier, est de maintenir un niveau d'exigence fort, notamment concernant le recours à des prestations qualifiées.

Concernant les sondes de détection, nous réexaminons actuellement cette question, non pas pour l'affaiblir, ce qui serait contraire à notre mission d'autorité nationale de cybersécurité, mais pour l'actualiser au regard de l'état de l'art.

Le cadre établi en 2013 se concentrait uniquement sur la détection réseau, c'est-à-dire l'analyse des flux entre le système d'information d'importance vitale et internet. Bien que toujours pertinente, cette approche n'est plus suffisante. Aujourd'hui, une stratégie de détection efficace doit combiner plusieurs sources : détection réseau, détection système et analyse de journaux. La France dispose heureusement de solutions dans tous ces domaines. En outre, pour la détection réseau, nous avons des sondes qualifiées par l'Anssi. Pour la détection système, il existe des outils de détection locaux, appelés EDR, comme ceux de la société HarfangLab, également qualifiés par l'Anssi. Ces éléments doivent être remis au goût du jour, et non pas démontés.

Un ajustement en termes de spécifications des exigences pourrait être réalisé. Toutefois, les principes fondamentaux resteront inchangés : le système d'information d'un opérateur d'importance vitale doit être supervisé et capable de détecter des attaques stratégiques émanant de services étatiques. Cela nécessite une détection de grande qualité et de confiance. Nous adapterons ces principes à l'évolution de l'état de l'art, avec potentiellement une obligation de résultat plutôt que de moyens, mais les consultations se poursuivent sur ce sujet.

M. le président Philippe Latombe. Je vous remercie. Nous examinerons la possibilité de répondre à la demande du rapporteur général de vous réentendre ultérieurement. Cependant, vous ne serez pas le dernier intervenant, car nous avons prévu d'auditionner en dernier lieu Mme la ministre chargée de l'intelligence artificielle et du numérique, ce qui servira de base à notre discussion générale. Nous avions le souhait de débuter ce cycle par votre audition, qui sera suivie par celle du SGDSN la semaine prochaine.

2. Audition de M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale (SGDSN), mardi 13 mai 2025 à 16 heures 30

Lors de sa réunion du mardi 13 mai 2024, la commission spéciale a auditionné M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale (SGDSN).

M. le président Philippe Latombe. Mes chers collègues, nous poursuivons les travaux de notre commission spéciale, qui ont commencé la semaine dernière avec l'audition de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (Anssi). Nous recevons aujourd'hui M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale (SGDSN), que je remercie de s'être rendu disponible.

Monsieur le secrétaire général, vous avez pris vos fonctions en mars dernier, après une carrière diplomatique qui vous a conduit à exercer des responsabilités éminentes, notamment en tant qu'ambassadeur de France en Iran. Le SGDSN s'inscrit dans une histoire ancienne. Né sous la III^e^ République, sous la forme du Conseil supérieur de la défense nationale, il a toujours eu pour vocation de répondre aux besoins de coordination interministérielle en matière de défense.

Depuis 2009, l'ajout du terme « sécurité » à son intitulé, à la suite du Livre blanc sur la défense et la sécurité nationale de 2008, a marqué un élargissement de ses missions à ce domaine essentiel. Aujourd'hui, le SGDSN couvre un champ stratégique étendu, qui concerne la défense, la sécurité, la programmation militaire, la dissuasion et la lutte contre le terrorisme. Dans son périmètre, on retrouve notamment Viginum, créé par le décret du 13 juillet 2021, chargé de la vigilance contre les ingérences numériques étrangères ; l'opérateur des systèmes d'information interministériels classifiés (OSIIC), initié par le décret du 21 avril 2020, et bien sûr l'Anssi, depuis le décret du 7 juillet 2009.

Le premier ministre est chargé de la mise en place du cadre général du dispositif de sécurité des activités d'importance vitale (SAIV), coordonné par le SGDSN. L'institution que vous dirigez depuis le début du printemps est donc particulièrement concernée par le projet de loi que la commission spéciale est chargée d'examiner. Le titre I^er^ du projet de loi vise en effet à transposer la directive 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, dite REC, et ainsi à actualiser et à modifier le dispositif de sécurité des activités d'importance vitale.

La directive REC, qui a été négociée sous la présidence française de l'Union européenne, s'inspire en grande partie du dispositif français existant. Ainsi, le nombre d'opérateurs d'importance vitale (OIV), qui est environ de 300, ainsi que le nombre de points d'importance vitale, de l'ordre de 1 500 ne devraient pas évoluer de manière significative. Pouvez-vous nous le confirmer ?

Toutefois, cette transposition marque un changement important de philosophie. Elle acte le passage d'une logique de protection des infrastructures d'importance vitale à une approche axée sur la résilience. Pourriez-vous nous éclairer par ailleurs sur les modalités de désignation des OIV et l'architecture de planification ? Ont-elles globalement vocation à être conservées par rapport au dispositif actuel ? Enfin, quelle est notre vision de l'article 16 *bis* qui traite du chiffrement ?

M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale. Je vous remercie pour votre invitation à m'exprimer devant votre commission aujourd'hui pour évoquer ce projet de loi relatif à la résilience des infrastructures et au renforcement de la cybersécurité. Comme vous l'avez rappelé, j'ai pris mes fonctions il y a un mois en arrivant directement depuis Téhéran et suis heureux d'évoquer avec aujourd'hui ce thème de la résilience, thème central pour les deux grandes missions qu'assure le SGDSN au profit du premier ministre, de l'ensemble du gouvernement et du président de la République : d'une part les travaux de coordination interministérielle dans le domaine de la défense et de la sécurité nationale, qui recouvre l'ensemble des questions de résilience nationale ; et d'autre part un certain nombre d'opérateurs d'agences qui dépendent directement du SGDSN.

Comme vous l'avez souligné, ce projet de loi porte sur la transposition de trois textes européens : la directive européenne sur la résilience des entités critiques, la directive *Network and Information Security 2* (NIS 2) et la directive *Digital Operational Resilience Act* (Dora). Ces trois textes forment un tout et constituent un ensemble d'innovations, mais aussi pour nous une certaine forme de continuité.

Je me félicite de la décision que vous avez prise collectivement de mettre en place une commission spéciale aux fins d'examen de ce projet, comme le Sénat l'avait fait avant vous. D'un point de vue technique, ces textes ne constituent pas un ensemble monolithique, mais un ensemble qui conserve toute sa cohérence. La directive REC reprend et développe, comme vous l'avez dit, monsieur le président, des principes bien connus en France : la politique de sécurité des activités d'importance vitale de la planification de défense et de sécurité nationale et la continuité d'activité en cas de crise.

Je ne m'appesantirai pas sur les titres II et III concernant la transposition de la directive NIS 2 ni sur la *lex specialis* qu'est la transposition de la directive Dora, puisque vous avez entendu le directeur général de l'Anssi sur la partie NIS 2 et que vous recevrez certainement le directeur général du Trésor concernant Dora.

La diversité de l'ensemble de ces textes justifie pleinement leur examen au sein d'une commission spéciale qui regroupe les compétences des commissaires de plusieurs commissions permanentes. Néanmoins, pour le gouvernement, pour l'ensemble des administrations et le SGDSN qui a coordonné une partie de ses travaux, ces textes témoignent d'une cohérence d'ensemble. Celle-ci se définit par l'objectif de la construction d'une meilleure résilience de notre pays face à des

menaces, y compris hybrides, des chocs et des crises de toute nature qui ne se tarissent pas.

Parmi l'ensemble de ces travaux, deux doivent être mentionnés en particulier : la revue nationale stratégique (RNS) en cours de finalisation, et la mise en œuvre de la stratégie nationale de résilience (SNR) qui, depuis avril 2022, évolue régulièrement et forme pour nous le cadre de la mise en place de ces directives et de la loi, lorsque vous aurez terminé vos travaux et que la loi sera formellement adoptée.

L'objectif consiste pour nous à faire face à des menaces de plus en plus agressives, des crises majeures qui touchent tous les secteurs d'activités de la vie de la nation, quelles qu'en soient les origines. La méthode se trouve en partie dans ce projet de loi qui fixe des cadres au sein desquels notre stratégie globale de résilience a vocation à se renforcer. Les actions seront mises en œuvre par l'ensemble des entités étatiques et publiques, mais aussi par un ensemble d'opérateurs régulés, en application des trois directives ainsi transposées. Au-delà de ces aspects techniques, ce projet de loi participe donc bien d'une entreprise générale collective de renforcement de la résilience de la nation en cas de crise.

Je termine ces quelques mots d'introduction en remarquant que, si en 2022, au sortir de l'épidémie de covid-19, le concept de résilience ne pouvait déjà plus être regardé comme une abstraction, force est de constater qu'il a pris aujourd'hui une nouvelle acuité et une nouvelle force, compte tenu de l'évolution de l'environnement stratégique. D'une certaine façon, nous avons été rattrapés par des réalités de plus en plus sombres et de plus en plus prégnantes pour l'ensemble des services de l'État. Je suis frappé, depuis je suis rentré de Téhéran et que j'ai pris mes fonctions, par l'affaissement des mécanismes internationaux de règlement des conflits, l'affaiblissement de l'idée de régulation, par les doutes qui peuvent naître sur les solidarités les mieux ancrées dans l'histoire, par l'inquiétude qui saisit les pays qui, comme le nôtre, demeurent attachés à l'idée que la paix vaut mieux que la guerre et que la coopération entre États est préférable au chantage. La prochaine actualisation de la RNS, en cours de pilotage interne par le SGDSN, permettra d'établir une synthèse de l'état du monde, de nos analyses de la menace et des risques, et surtout des voies et moyens que la France doit choisir pour y faire face.

Je souhaite tout d'abord évoquer le contexte dans lequel s'inscrit le projet de loi, c'est-à-dire l'actualisation de la RNS que le président de la République nous a commandée dans ses vœux aux armées, le 17 janvier dernier. Ceux qui parmi vous siègent habituellement au sein de la commission de la défense et des forces armées sont bien informés de ce travail en cours.

Je rappelle la manière dont le président de la République a décrit la situation à l'entame de son adresse à nos compatriotes, le 5 mars : *« Vous êtes en effet légitimement inquiets devant les événements historiques en cours qui bouleversent l'ordre mondial. La guerre en Ukraine, qui a entraîné près d'un million de morts et de blessés, continue avec la même intensité. Les États-Unis d'Amérique, notre allié,*

ont changé leur position sur cette guerre, soutiennent moins l'Ukraine et laissent planer le doute sur la suite. Dans le même temps, les mêmes États-Unis d'Amérique entendent imposer des tarifs douaniers aux produits venant d'Europe. Enfin, le monde continue d'être sans cesse plus brutal, et la menace terroriste ne faiblit pas. Au total, notre prospérité et notre sécurité sont devenues plus incertaines. Il faut bien le dire, nous entrons dans une nouvelle ère. ».

Le 3 mars, devant vous, lors d'une déclaration du gouvernement sur la situation en Ukraine et la sécurité de l'Europe, le premier ministre a quant à lui évoqué « *une situation historique qui est à nos yeux la plus grave, la plus déstabilisée et la plus dangereuse de toutes celles que notre pays et notre continent ont connues depuis la fin de la seconde guerre mondiale.* ».

Nous faisons donc face à nous à un environnement international profondément dégradé, profondément menaçant. Cette dégradation est liée à une série de facteurs, à une série d'actions d'États. Nous pensons évidemment en premier lieu à la Russie, mais bien au-delà, à l'ensemble des évolutions de l'environnement stratégique. Plus précisément sur notre territoire, les modes d'action que nous disons hybrides sont employés aujourd'hui par un certain nombre de nos adversaires et sont devenus une forme d'agacement sinon quotidien, du moins courant. Je rappelle de quoi nous parlons : les étoiles de David sur les murs du 14e arrondissement ; les mains rouges sur le mémorial des Justes ; les cercueils en carton sous la tour Eiffel ; les réseaux de faux comptes qui bombardent les plates-formes numériques d'histoires inventées et d'informations déformées, des attaques cyber.

Nos partenaires européens comme les pays baltes, la Pologne, l'Allemagne, le Royaume-Uni, la Roumanie font aussi l'objet de manœuvres d'intimidation, d'agression, de cyberattaques, d'incendies criminels. Chaque échéance électorale est mise à profit pour mobiliser un écosystème de manipulation de l'information et d'ingérence numérique étrangères qui pèse sur le fonctionnement de nos démocraties.

En raison de l'agressivité russe, qui n'a rien de neuf et qui s'inscrit dans une longue durée, et de l'incertitude qui pèse sur un certain nombre de mécanismes de solidarité, nous sommes aujourd'hui collectivement amenés à réviser nos scénarios centraux, en particulier l'hypothèse d'un engagement majeur de nos forces armées. Depuis plusieurs décennies, nous envisagions des opérations de projection de puissance, de projection de forces, loin du territoire métropolitain. Nous sommes désormais obligés d'envisager la mobilisation de nos forces armées dans un conflit de haute intensité, en dehors du territoire national, mais dans la périphérie de l'Europe.

Cela change beaucoup de choses dans l'approche de certaines questions comme les réserves, les stocks stratégiques, les capacités industrielles, la mobilisation des forces morales de la nation. Face à cette hypothèse d'engagement, nous devons aussi durcir notre capacité à agir et notre capacité à faire face aux chocs

que nous sommes amenés à subir. Le projet de loi qui vous est soumis concourt directement à cet objectif, qui est au cœur des travaux de la RNS. Les infrastructures critiques qui sont déjà soumises aux risques naturels comme le dérèglement climatique ou les épidémies sont aujourd'hui régulièrement la cible d'attaques physiques et cybernétiques. Je pense ici à des incendies volontaires de pylônes de télécommunications, des sabotages commis contre le réseau ferré, des cyberattaques contre les hôpitaux. Le retour des conflits de haute intensité sur le continent européen et aux frontières de l'Europe a mis en lumière la vulnérabilité des infrastructures critiques, qui constituent aujourd'hui des cibles prioritaires et stratégiques en cas de conflit. Leur destruction peut engendrer de graves conséquences en France et dans les États voisins, du fait de l'interdépendance structurelle de nos sociétés dans les secteurs critiques.

Cette multiplication des risques et menaces a ainsi conforté une ambition politique et normative sur la protection de ces infrastructures critiques, qui se matérialise dans le titre I^{er} du projet de loi. L'ambition qui vous est soumise consiste à améliorer la fourniture, en Europe, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales, en renforçant la résilience des opérateurs d'importance vitale nommés « *entités critiques* » dans la directive.

Pour être complet, je veux vous indiquer que le travail d'actualisation en cours traitera d'une forme de réarmement de la défense civile de notre pays – j'ai évoqué les forces morales. Le concept central de ce réarmement est la résilience ; celle, individuelle et collective, de nos concitoyens, mais aussi celle des organisations. Nos orientations stratégiques vis-à-vis des institutions internationales, de nos alliances, de nos partenaires et de nos compétiteurs, sont aujourd'hui organisées autour de ce concept de résilience.

Le deuxième point sur lequel je souhaite revenir concerne précisément l'État actuel de notre stratégie nationale de résilience. En effet, je ne voudrais pas donner l'impression que la question de la résilience ne serait liée qu'à des phénomènes récents, intervenus ces derniers mois. La politique de sécurité des activités d'importance vitale qui vise à assurer la protection et la « continuité d'activité » de l'ensemble des opérateurs indispensables au fonctionnement de nos institutions, de notre économie, et à notre sécurité, date de 2006. On ne parlait pas de résilience à l'époque, mais il s'agit bien de cela.

Plus près de nous, le SGDSN a été mandaté par le premier ministre Jean Castex en mai 2021 pour préparer une stratégie nationale de résilience. Cette consigne visait à faire fructifier un certain nombre d'enseignements tirés de la pandémie de covid-19. La stratégie nationale de résilience a été validée par Matignon en avril 2022. Depuis lors, elle est à la fois en cours de déclinaison par les ministères, mais aussi d'ajustement permanent à l'évolution de notre environnement stratégique et des besoins qui se font jour.

De façon générale, cette SNR repose sur un ensemble de soixante-treize actions qui concourent à trois objectifs stratégiques : la préparation en profondeur

de l'État aux crises, le développement des capacités humaines et matérielles pour y faire face et l'adaptation de la communication publique aux enjeux de la résilience. Sur la base de ces soixante-treize actions, un certain nombre d'objectifs et d'indicateurs sont déclinés depuis 2022. Ce triptyque constitue l'une des matérialisations de la stratégie nationale de résilience. Il s'agissait à l'époque à la fois de promouvoir une polyvalence des outils de gestion de crise, mais aussi d'installer le concept de résilience au cœur de nos travaux de planification. À ce titre, une des tâches du SGDSN consiste à préparer la planification nationale de défense et de sécurité nationale.

Nous avons donc complété le dispositif intérieur des grands plans qui visait à répondre à une menace ou un type de menace – vous connaissez d'ailleurs tous le plus célèbre d'entre eux, le plan Vigipirate – avec des fiches mesures universelles, non pas par type de catastrophes, mais par type de conséquences. Ces plans possèdent de grandes qualités, mais, à l'usage de vingt années de gestion de crises diverses, il est apparu, notamment en 2020, qu'ils comportaient également des inconvénients. Ainsi, ils sont bien construits et très complets, mais aussi lourds à mettre en œuvre et complexes à mettre à jour. Le choix effectué en 2021 dans le cadre de la SNR a donc consisté à envisager la planification et la gestion de crise de façon plus générique, en créant une forme de « tronc commun » à l'ensemble des crises et à y associer un ensemble de mesures de mise en œuvre dont le choix permet de s'adapter à la typologie de la crise, qu'elle soit sanitaire, industrielle, climatique, sécuritaire, de manipulation ou de guerre économique.

Autrement dit, nous avons été guidés par un souci de simplification de l'ensemble de travaux de planification nationale de défense et de sécurité nationale. Cette simplification en cours se poursuit puisque nous sommes aujourd'hui rentrés dans sa deuxième phase. De plus, cette SNR se recentre sur deux grands objectifs qui permettent d'offrir plus de clarté et de pilotage à l'ensemble de la stratégie.

Ce recentrage se concentre premièrement sur un objectif très simple : assurer la continuité de la vie économique de la nation. J'entends par là l'impératif d'assurer la résilience des réseaux essentiels (téléphonie d'urgence, eau, gaz, électricité, énergie, communications, communications classifiées) et de remédier aux vulnérabilités critiques d'approvisionnement qui, trop souvent, placent notre pays dans une situation de vulnérabilité, si ce n'est de dépendance.

La deuxième grande priorité consiste à mobiliser les citoyens au service de la résilience et de la défense globale. Cela signifie très concrètement les former, les sensibiliser, les éduquer dès le plus jeune âge et tout au long de la vie. Cela implique également d'harmoniser et de simplifier les dispositifs existants de réserve. Cela nous engage enfin à encourager et faciliter toutes les bonnes volontés, c'est-à-dire tous nos concitoyens et nos compatriotes qui souhaitent aider et favoriser l'engagement, quel qu'il soit, pour constituer un vivier de volontaires mobilisables en cas de crise.

Cette stratégie nationale de la résilience constitue donc la déclinaison opérationnelle de tous les ministères et, au-delà, de toutes les collectivités publiques, de ce que nous caractérisons, dans le cadre de la RNS, comme l'adaptation nécessaire de nos outils et de nos planifications à une évolution drastique de la menace, et notamment des menaces hybrides qui pèsent sur le territoire national.

J'en viens au troisième et dernier point, qui constitue le cœur de vos travaux et en particulier du titre Ier de la loi. Le constat de départ, qui a motivé l'adoption de la directive REC, porte précisément sur la multiplication des risques et des menaces pouvant affecter nos infrastructures critiques, c'est-à-dire celles qui sont nécessaires à l'exercice d'une activité d'importance vitale ou dont une perturbation pourrait mettre gravement en cause la santé de la population ou l'environnement.

La directive REC complète donc la démarche engagée par l'adoption de la directive de décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'étendre leur protection, alors limitée aux secteurs des transports et de l'énergie, aux opérateurs de dimension européenne. L'ambition de REC consiste désormais à améliorer la fourniture, dans le marché intérieur européen, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales en renforçant la résilience des opérateurs d'importance vitale, désignés comme « entités critiques » dans la directive.

La directive, qui devait être transposée en droit national le 17 octobre 2024 au plus tard, assure un socle minimal commun de résilience à tous les opérateurs de l'Union européenne (UE). Incidemment, elle permet d'atténuer une forme de *dumping* des obligations sécuritaires entre États membres, le cadre français étant déjà relativement complet au regard des dispositions de la directive.

En France, nous avons fait le choix de la simplicité et de la continuité : la transposition révise le dispositif national de sécurité des activités d'importance vitale défini dans le code de la défense (articles L. 1332-1 et suivants), qui a fait ses preuves. Cette politique publique, qui trouve ses origines dans une ordonnance de 1958, instaurée formellement à compter de 2006, a prouvé son efficacité et fait l'objet d'une déclinaison sur l'ensemble du territoire national. Il y a donc lieu de se féliciter de ce que les contours de la directive REC coïncident presqu'exactement avec ceux de la SAIV nationale.

Cette réforme normative et doctrinale représente aussi pour nous l'occasion de moderniser notre dispositif national : révision de la classification du dispositif (statut d'OIV) et renforcement de la mise en œuvre et de la coordination du dispositif, dans une logique de cohérence, d'efficacité et de simplification.

La transposition s'inscrit donc bien dans une politique de résilience globale et cohérente : les OIV seront également soumis aux obligations de cyber-résilience prévues par la directive NIS 2 (négociée en parallèle de la directive REC et de la

directive Dora portant sur la résilience du secteur financier). La cohérence d'ensemble que j'évoquais en introduction n'est donc pas une vue de l'esprit.

L'identité de vue entre la directive et le dispositif national constitue évidemment un avantage à plusieurs égards. Le vocabulaire national est conservé, de même que la logique d'identification des sites les plus sensibles – les points d'importance vitale – ainsi que la planification associée.

Le suivi effectué par le SGDSN, les ministères coordonnateurs, les zones de défense et de sécurité et les préfets de département est maintenu et pourra être renforcé. J'y veillerai personnellement. D'ores et déjà, j'ai décidé de poursuivre l'œuvre de sensibilisation des préfets territoriaux à l'ensemble des aspects de la stratégie nationale de résilience. Je suis notamment intervenu lors de la dernière réunion des préfets au ministère de l'intérieur et me déplacerai dans les zones de défense pour poursuivre cette sensibilisation visant à contribuer à l'appropriation par l'ensemble des acteurs territoriaux de ce concept de résilience.

Autre avantage important pour les opérateurs d'importance vitale, nombre des exigences de la directive sont déjà mises en œuvre à travers le dispositif actuel. Ainsi, les entités concernées par la révision du dispositif SAIV sont les opérateurs qui étaient déjà assujettis au dispositif existant.

De nouveaux opérateurs d'importance vitale pourraient le cas échéant être désignés au titre de leurs activités, considérées comme d'importance vitale par l'État si celles-ci devaient évoluer ou émerger, en particulier dans les secteurs de l'assainissement, de l'hydrogène, ainsi que les réseaux de chaleur et de froid, nouvellement identifiés par la directive REC. Toutefois, le nombre d'opérateurs d'importance vitale, autour de 300 aujourd'hui, n'a pas vocation à augmenter significativement.

Concrètement, la mise en œuvre de la directive devrait se traduire par un certain nombre d'améliorations. Il s'agit d'abord d'une meilleure prise en compte des interdépendances entre les secteurs, et entre les États membres, avec l'identification par les opérateurs de leurs interdépendances et de leurs chaînes d'approvisionnement dans une logique de continuité d'activités. Il s'agit ensuite d'une obligation de notification des incidents majeurs, qui existe déjà dans le domaine de la cybersécurité, mais aussi d'une évolution et d'un renforcement du dispositif d'enquêtes administratives de sécurité. Enfin, l'amélioration porte sur une révision du dispositif de sanctions pour les opérateurs qui ne respecteraient pas leurs obligations, avec la création d'un régime de sanctions administratives, en lieu et place des sanctions pénales existantes. Ces quatre mesures nous permettront de mettre en œuvre notre stratégie nationale de résilience de façon beaucoup plus efficace que par le passé.

Pour sa part, la création d'un nouveau statut d'« *entité critique d'importance européenne particulière* » (ECIEP) pour les opérateurs fournissant un service essentiel à au moins six États membres de l'UE, porte des enjeux

particuliers, soit une obligation de notification à la Commission et de partage d'information avec les États membres concernés. Néanmoins, il convient de souligner que cette directive a été négociée – le SGDSN a été particulièrement vigilant sur ce point – dans l'objectif de respecter les prérogatives nationales et les enjeux de souveraineté, de sécurité et de protection du secret afférents à la protection des infrastructures critiques, de sorte que seules les données agrégées seront transmises à la Commission européenne.

Dans une optique de modernisation et de cohérence de l'ensemble du dispositif, le choix a été opéré de donner la possibilité à l'autorité administrative d'autoriser les opérateurs à déroger, dans certains cas précis, au droit commun de la commande publique, lorsqu'il pourrait être porté atteinte aux intérêts essentiels de l'État.

Je souhaite enfin évoquer le coût des mesures imposées. Trois points me semblent devoir être précisés. En premier lieu, ces mesures pourront engendrer un coût pour un certain nombre d'opérateurs. Ensuite, nous ne sommes pas en mesure aujourd'hui d'évaluer exactement le coût afférent à l'évolution de ce dispositif, en raison à la fois de la variété des secteurs et des opérateurs couverts par notre stratégie de résilience. Troisièmement, le coût des mesures de continuité d'activité n'est évidemment en rien comparable au coût d'un arrêt d'activité. Nos opérateurs économiques le savent déjà parfaitement : ils n'ont pas attendu l'État, pour la plupart d'entre eux, pour investir dans la sécurisation de leurs activités. Nous allons donc apprendre en marchant, mais je crois que la question du coût doit être abordée avec sérénité.

J'en termine par les collectivités territoriales, qui dans la directive REC – contrairement à NIS 2 qui s'appliquera directement à un certain nombre de collectivités locales –, ne constituent pas un secteur spécifique. Certaines collectivités sont incluses dans le champ de la directive REC ; il s'agit de celles qui sont déjà désignées OIV, car elles assurent des activités d'importance vitale ou services essentiels au sens de la directive REC – dans les secteurs qui relèvent de leur compétence ; par exemple pour les secteurs de la gestion de l'eau, des transports et de l'énergie.

Dans le cas d'une délégation de service public (DSP) pour des activités d'importance vitale, le projet de loi « Résilience » prévoit l'information de la collectivité territoriale afin que celle-ci soit en mesure de prendre en compte les implications du dispositif sur son délégataire. Ainsi, le délégataire est tenu de mettre en place des mesures pour assurer la résilience de son activité, notamment la sécurisation des sites sans lesquels il ne peut exercer son activité d'importance vitale.

Pour être totalement complet, de nouvelles collectivités territoriales pourraient être désignées à l'avenir au titre de leurs compétences dans les secteurs de l'assainissement, de l'hydrogène, ainsi que des réseaux de chaleur et de froid,

car il s'agit de secteurs nouveaux visés par la directive REC et par le projet de loi de transposition.

Tels sont les éléments que je voulais vous transmettre concernant nos travaux dans le cadre de notre analyse des menaces et des risques qui pèsent, de notre travail sur la RNS ; mais aussi de nos actions depuis 2022 en termes de mise en œuvre et de modernisation de la SNR. Les dispositions spécifiques du titre Ier du projet de loi viennent parfaitement s'intégrer selon nous dans ce besoin de durcissement et de modernisation d'activités qui sont essentielles à la continuité de la vie de la nation.

M. le président Philippe Latombe. Je cède la parole aux rapporteurs pour une première série de questions.

M. Éric Bothorel, rapporteur général. Monsieur le secrétaire général, puisque vous étiez, il y a encore quelques semaines, notre ambassadeur auprès de la république islamique d'Iran, je ne peux résister à l'envie de vous poser une question qui n'a rien à voir avec le projet de loi, mais qui est également très liée à la thématique de la résilience. J'ai bien conscience que nos auditions sont publiques, que vos réponses sont par nature mesurées, mais je souhaite à titre personnel vous interroger sur la situation des otages Cécile Kohler et Jacques Paris en Iran. Quelle est votre lecture de ce qui semble être une politique qui touche près d'une vingtaine d'Européens et que l'on peut qualifier de politique « d'otages d'État » ?

Je reviens maintenant sur le sujet qui nous réunit aujourd'hui, le projet de loi. D'abord, quelles sont selon vous les nouvelles menaces qui pèsent sur les infrastructures ? Quelles sont les infrastructures qui vous semblent aujourd'hui les plus sensibles ? Je pense notamment aux gazoducs, aux menaces sous-marines, bactériologiques et celles portant sur les réseaux d'eau.

Nous passons de la notion d'opérateurs de services d'importance vitale, qui étaient parfois uniques et très centralisés, à un élargissement du nombre d'acteurs concernés, avec des entités territoriales nombreuses, des acteurs publics comme privés. Selon vous, l'organisation du SGDSN, par nature très centralisée auprès du premier ministre, devra-t-elle s'adapter à cet élargissement territorial ? Les territoires ultramarins devraient-ils connaître, selon vous, une organisation et une réglementation différenciées ?

Je m'associe également à la question du chiffrement, évoquée par le président Latombe. Ce sujet, qui nous préoccupe tous, est aujourd'hui intégré dans le texte. Vous semble-t-il nécessaire que nous consolidions et que nous sécurisions le chiffrement de bout en bout dans une forme de sacralisation d'une rédaction qui pourrait être plus parfaite ?

Un débat parallèle voit aussi le jour concernant le renseignement d'origine sources ouvertes ou *open source intelligence* (Osint). Selon vous, est-il nécessaire de légiférer sur l'Osint et de profiter de l'opportunité de ce texte pour le faire ?

Enfin, nous savons de longue date que les services télécoms ne sont pas au rang des services essentiels dans notre pays. En tant que Breton, je constate que lorsqu'une tempête survient, les priorités portent surtout – de manière légitime – sur le rétablissement de l'eau potable, les hôpitaux, les personnes sous assistance respiratoire, mais les télécoms sont souvent relégués au second plan. Ne faudrait-il pas, dans ce texte, rehausser les infrastructures télécoms au rang des services essentiels, afin que leur remise en route constitue également une priorité ?

Mme Catherine Hervieu, rapporteure. Depuis plusieurs années, les activités françaises représentent une cible pour des États et acteurs étrangers. Nous avons pu évoquer différents points de vigilance, notamment lors de la consultation des parlementaires pour la révision de la RNS 2022. Collectivement, nous demandons la rédaction d'un Livre blanc sur la sécurité et la défense pour une réelle stratégie nationale.

Pour autant, une partie des parlementaires reste encore à convaincre et une majorité des Français à informer. L'information est la clé de voûte pour éclairer, mais également influencer. Notre calendrier est restreint, et soyons réalistes, nous sommes en retard. J'ai d'ailleurs exprimé l'urgence de traiter ce projet de loi en priorité lors des questions au gouvernement, le 30 avril dernier. Dans le rapport de la direction générale de la sécurité intérieure (DGSI) et de la direction générale de la sécurité extérieure (DGSE) qui a fuité, il est indiqué que « *La Russie mène des actions offensives qui peuvent avoir des conséquences directes sur la vie des Français : tentatives d'incendie de centres commerciaux, attaques sur des câbles sous-marins, de télécommunications, cyberattaques sur des terminaux satellitaires (…) visant à faire dysfonctionner des infrastructures critiques, fragiliser l'organisation de la société ou espionner des entités françaises* ». Nos objectifs actuels consistent donc à réduire nos vulnérabilités et à être résilients.

Pourtant, nous sommes tous témoins d'ores et déjà d'ingérences sur nos territoires dans les administrations, les hôpitaux, les communications, les entreprises. Au-delà de la sensibilisation, l'information de l'ensemble des Français, des élus et des opérateurs est nécessaire. Les acteurs de nos territoires disposent néanmoins de moyens différents pour faire face aux menaces dont ils sont les cibles.

Vous avez évoqué les collectivités territoriales et la façon d'organiser les DSP, mais il faudra également tenir compte des différences qui existent entre les territoires. Comment répondre à ces impératifs de protection avec les moyens humains et financiers dont nous disposons actuellement ? Ce projet de loi demande un renforcement et une augmentation des moyens pour sa mise en œuvre.

Il nous faudra développer et cibler les besoins prioritaires à développer, et nous devrons hiérarchiser les différentes étapes du calendrier, compte tenu des situations que vous avez décrites. Concernant le titre I^er^, dont je suis rapporteure, pourriez-vous développer l'application du dispositif aux opérateurs régaliens, exclus de la direction en droit européen et intégrés au dispositif français de sécurité des activités d'importance vitale ?

Madame Anne Le Hénanff, rapporteure. Monsieur le secrétaire général, que pensez-vous du critère du nombre d'habitants retenu pour qu'une collectivité soit considérée comme une entité essentielle, et en particulier du seuil arrêté par le Sénat, c'est-à-dire 30 000 habitants ? Que pensez-vous de la classification des collectivités comprenant moins de 30 000 habitants dans la catégorie des entités importantes ?

Par ailleurs, un certain nombre d'administrations sont exclues du périmètre d'application du projet de loi, notamment celles exerçant dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, les missions diplomatiques et consulaires françaises, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), les ministères, le Sénat et l'Assemblée nationale. Dans quelles mesures ces exemptions se justifient-elles ? Quelles garanties pouvez-vous nous apporter quant à leur degré de cybersécurité et de cyber-résilience ?

Ensuite, vous avez parlé de l'implication des préfets. Je fais partie de ces députés qui, depuis des années, demandent que les préfets s'impliquent davantage dans l'accompagnement à la montée en cybersécurité des territoires. Je suis donc particulièrement intéressée par les propos que vous avez tenus à ce propos. Vous avez parlé particulièrement des zones de défense, mais qu'en est-il des autres territoires qui n'en sont pas ? De quels moyens vont-ils disposer ? Quelles seront les marges de manœuvre des collectivités locales, des hôpitaux ?

Enfin, le budget du SGDSN a diminué en 2025. L'Anssi, l'OSIIC et Viginum ont ainsi vu leurs moyens diminuer de 8 millions d'euros. Alors que nous allons entamer l'étude de la loi « Résilience » et la transposition de la directive NIS 2, comment pourrons-nous agir, compte tenu de cette réduction de budget ?

M. Mickaël Bouloux, rapporteur. Je suis, pour ma part, rapporteur thématique en ce qui concerne le titre III du projet de loi, qui porte sur la résilience opérationnelle numérique du secteur financier et qui transpose la directive Dora.

Je souhaite vous poser des questions plutôt générales sur le rôle du SGDSN dans la résilience des entités financières. Tout d'abord, quels sont vos relations et vos leviers d'action avec le secteur bancaire ? J'ai lu qu'il existait un réseau de référents désignés en coordination avec la Fédération bancaire française, afin de favoriser le financement privé de la base industrielle et technologique de défense (BITD), mais aussi de développer une culture de défense chez ces acteurs privés.

Ces référents pourraient-ils jouer un jour un rôle dans la résilience opérationnelle numérique du secteur financier ? Les acteurs bancaires constituent-ils des cibles de choix pour les tentatives d'ingérence étrangère, dans le but de déstabiliser notre économie ? Enfin, quels types de menaces cyber certains États sont-ils susceptibles de mettre en œuvre contre nos entités financières ?

M. Nicolas Roche. Monsieur le rapporteur général, nos autorités politiques, le président de la République, le premier ministre et le ministre de l'Europe et des affaires étrangères ont été parfaitement clairs depuis des mois – si

ce n'est des années – sur le statut d'otages d'État de Cécile Kohler et Jacques Paris. Je suis personnellement allé assister les familles des otages, dont celles de ceux de nos otages qui ont pu rentrer en France ; lesquels sont heureusement nombreux. Nous avons célébré tristement la semaine dernière les trois années de détention arbitraire de ces deux otages aux mains de la république islamique d'Iran. Ils constituaient la priorité de mon action pendant trois ans à l'ambassade de France en Iran. Je reste mobilisé, comme tous les services de l'État et comme le président de la République l'a encore rappelé, pour faire en sorte qu'enfin, nos compatriotes puissent rentrer en France.

Ensuite, s'agissant de la question du chiffrement, nous avons besoin de temps et de sérénité pour mener un travail technique très approfondi, interne aux services de l'État, pour traiter au fond ce sujet, de façon professionnelle, méthodique, propre, détaillée. Nous reviendrons ensuite vers le gouvernement et le président de la République pour signaler si des solutions techniques sont possibles, leurs avantages et inconvénients, afin qu'une décision puisse être prise en toute connaissance de cause. Cette question est évidemment incontournable, puisqu'elle concerne plusieurs politiques publiques essentielles, fondamentales.

S'agissant des éléments plus directement liés au titre I^er^, c'est-à-dire la nature et l'identification des menaces prioritaires, nous n'avons malheureusement pas le luxe du choix. Nous ne définissons pas ces menaces et les risques, qui nous sont souvent imposés par nos adversaires. L'évolution de l'environnement stratégique de ces dernières années montre que, factuellement, les menaces qui ont eu à un moment ou à un autre, en France ou dans des pays amis, un impact direct sur la continuité de la vie de la nation, ont touché tous les secteurs possibles.

Dans le domaine cyber, elles concernent à la fois l'espionnage et les manipulations de l'information, qui sont de plus en plus complexes, de plus en plus élaborées technologiquement, et qui visent de plus en plus le cœur du fonctionnement de nos sociétés. Elles visent aussi le sabotage physique d'un certain nombre d'activités, y compris d'importance vitale. Un certain nombre de secteurs d'activités ont ainsi été touchés en France et en Europe ces dernières années. Elles portent également sur la guerre économique et commerciale, le *lawfare*, c'est-à-dire l'instrumentalisation du droit à des fins de disruption des relations internationales.

Aujourd'hui, nous n'avons pas le luxe de choisir ou prioriser les menaces qui pèsent sur la continuité de la vie de la nation et nous devons toutes les prendre en compte. La RNS réalisera une description précise de l'ensemble de ces menaces sur cette partie du scénario, qui concerne le volet des menaces hybrides, qui pèsent sur le territoire national. Le ciblage très précis qui a été opéré jusqu'à présent sur les secteurs prioritaires pour la continuité de la vie de la nation – et qui ne devrait pas être bouleversé – indique ce que la nation doit protéger, *minimum minimorum*.

Ensuite, je crois que l'existence même du SGDSN, son double rôle d'animation interministérielle et d'opérateur dans un certain nombre de secteurs, de façon centralisée auprès du premier ministre, constitue une immense chance pour

notre système administratif et politique. Nous ne sommes pas pour autant inattentifs à la décentralisation, aux collectivités territoriales, aux acteurs privés, aux associations, à nos compatriotes. Cependant, l'environnement stratégique auquel nous sommes soumis impose une forme de centralisation de l'analyse de la menace, de la planification de défense et de l'animation du collectif de la sécurité nationale et de la résilience.

Le SGDSN ne fait pas tout lui-même, très loin de là. Il joue un rôle essentiel dans ce domaine-là d'animation des travaux interministériels et d'animation de l'ensemble des acteurs publics, mais aussi privés. Par ailleurs, dans des domaines très spécifiques qui nous ont été confiés, il endosse un rôle d'opérateur opérationnel dans des secteurs essentiels pour la résilience de la nation, à travers l'Anssi, Viginum et l'OSIIC. En résumé, j'estime que cette organisation et ce pilotage central du SGDSN constituent une des valeurs ajoutées de notre dispositif. Certains pays européens souffrent *a contrario* d'un manque de coordination interministérielle dans la mise en œuvre d'une véritable stratégie de résilience.

Ensuite, il ne me semble pas nécessaire de développer un cadre juridique dédié à l'outre-mer. En revanche, il existe le besoin d'une prise en compte particulière des opérateurs et des situations spécifiques de nos territoires ultramarins, qui sont soumis à des natures et des types de menaces hybrides singulières, dans la mise en œuvre de l'ensemble de nos plans de résilience.

Je me permets de réserver ma réponse sur l'Osint. Je fais partie de ceux qui pensent depuis longtemps que cette question est centrale et que nous avons besoin de capacités d'*open source*. Je reviendrai vers vous plus spécifiquement sur cette question.

Il serait erroné de considérer que les réseaux de télécommunication sont par essence secondaires. En tant que secrétaire général de la défense et de la sécurité nationale, je préside un comité interministériel chargé en partie de la supervision des communications d'urgence. Il existe bien un impératif de rétablissement très rapide des communications d'urgence au minimum pour assurer la continuité de la vie de la nation. Par ailleurs, un certain nombre d'éléments centraux des grands opérateurs de réseaux téléphoniques font partie des systèmes intégrés à notre stratégie nationale de résilience ; nous leur imposons un certain nombre d'obligations.

S'agissant de l'information sur les menaces et de la sensibilisation, je partage entièrement votre évaluation, madame Hervieu. L'un des objectifs de la RNS consiste précisément à contribuer à cette prise de conscience collective et à cet effort pédagogique d'éducation et de sensibilisation de tous nos compatriotes concernant l'ensemble des menaces, notamment hybrides, des risques ou des hypothèses d'engagement majeur de nos forces armées dans une guerre potentielle.

À ce titre, après trois ans passés à l'étranger, je retrouve des compatriotes et des concitoyens dont la prise de conscience est plus mûre que lorsque j'ai quitté la

France en 2022, s'agissant de la menace cyber, de la menace de manipulation de l'information, de la menace de guerre commerciale, de sabotage et d'espionnage. Cependant, je vous rejoins entièrement sur le fait que nous ne sommes pas encore aujourd'hui là où nous devrions être et que l'effort de sensibilisation et de renforcement doit être poursuivi. Il s'agit d'ailleurs d'un des objectifs de la RNS, raison pour laquelle j'ai demandé et obtenu de mes autorités politiques un délai supplémentaire pour permettre la poursuite des consultations, en particulier avec les commissions de la défense de l'Assemblée nationale et du Sénat, dans l'élaboration de cette RNS. La publication et la diffusion de la RNS seront marquées par un effort très vaste d'éducation et de sensibilisation à partir de la synthèse de l'évaluation de la menace et des risques qui pèsent sur le territoire, à l'horizon des années 2030-2040.

Ensuite, toutes les infrastructures sont sensibles en réalité ; je ne peux pas vous répondre différemment : à partir du moment où un opérateur d'importance vitale a été qualifié comme tel, nous ne pouvons pas établir de hiérarchie entre eux. La logique profonde de notre cadre politique, juridique et stratégique consiste précisément à adopter une cohérence d'ensemble de notre stratégie de résilience qui suppose que tous les OIV, toutes les activités d'importance vitale qui ont été identifiés soient protégés, non plus dans une logique de protection de points ponctuels, mais dans une logique de continuité d'activité et de résilience.

À partir du moment où des opérateurs, des activités ou des points entrent dans le champ de la directive REC, du dispositif de la loi « Résilience » et de nos plans de défense, il revient aux opérateurs de se mettre en conformité avec ces obligations qui, encore une fois, sont essentielles pour la continuité de la vie de la nation.

Madame la rapporteure, au-delà des collectivités territoriales et de l'ensemble des acteurs, de nos compatriotes, de nos concitoyens et du tissu associatif, il existe un impératif de mobilisation, qui rejoint d'ailleurs la question de la sensibilisation. Au niveau central, dans les administrations de l'État, en particulier celles qui relèvent directement de la défense et de la sécurité nationale, le niveau de prise de conscience et de connaissance est élevé. J'ai déjà eu l'occasion de vous indiquer qu'il l'est également chez nos compatriotes. Entre les deux, cette prise de conscience est inégale chez un certain nombre d'acteurs pourtant essentiels à la résilience de la nation.

La mobilisation que vous mentionnez est donc bien nécessaire. Elle interviendra en particulier à travers la publication et la mise en œuvre de la RNS. C'est la raison pour laquelle je suis intervenu devant l'ensemble des préfets, pour les sensibiliser sur le scénario central de la RNS, les impératifs de la stratégie nationale de résilience et de mise en œuvre, et la nécessaire mobilisation de l'ensemble des acteurs de l'État et, au premier chef, des préfets et de l'ensemble des acteurs déconcentrés de l'État. Ils jouent un rôle essentiel en tant qu'animateurs de l'ensemble des écosystèmes territoriaux qui contribuent à la défense et à la sécurité

nationale, y compris les collectivités territoriales. Il est impératif de multiplier les instances et les enceintes dans lesquelles il nous faut mener cette discussion.

Traditionnellement, tous les Livres blancs et les RNS comportent une dimension nationale d'explication et une déclinaison internationale, afin d'expliquer à nos partenaires étrangers ce que nous réalisons et de construire des coopérations internationales. Le travail est spécifique cette année : nous devrons ajouter à ces deux dimensions une innovation très importante, qui concernera une partie territoriale de la déclinaison de la RNS, à travers la mobilisation des acteurs locaux. Sauf erreur de ma part, la question du seuil démographique pour les entités et des exemptions dans certains secteurs relève très directement de la partie consacrée au cyber et à NIS 2, et non du titre I^{er} sur la résilience.

Concernant les efforts budgétaires, je ne peux que concourir à votre évaluation : la mise en œuvre de la SNR et de la stratégie nationale de cybersécurité nécessitera un certain nombre de décisions. Il reviendra évidemment au gouvernement d'assurer le bouclage de l'ensemble de nos priorités. Interviendra alors, comme dans tout processus budgétaire classique, une mise en adéquation entre les mesures que nous avons identifiées et les contraintes financières, dans un cadre budgétaire qui me dépasse très largement. Ma responsabilité consiste à porter auprès de mes autorités politiques des choix clairs, et en particulier des priorités en matière de résilience et de sécurité nationale, impliquant des choix budgétaires en termes de ressources humaines. Les choix relèvent ensuite des autorités politiques et du Parlement, en toute connaissance de cause.

Monsieur Bouloux, je suis moins familier de la dimension bancaire. Sur ce sujet, Bertrand Dumont, le directeur général du Trésor constituera un interlocuteur précieux. Je peux néanmoins confirmer l'existence de relations spécifiques entre le SGDSN et les grands acteurs bancaires et assuranciels pour garantir, dans la durée, le financement et l'existence de la BITD. Je ne rentrerai pas davantage dans les détails à l'occasion de cette session publique ; il en sera de même concernant les ingérences étrangères.

Cependant, il est évident que les menaces, en particulier cyber, concernent la totalité des secteurs. Dès lors, il n'y a aucune raison, *a priori*, de considérer que le secteur bancaire n'est pas lui aussi une cible potentielle, compte tenu de son degré de sensibilité aux questions technologiques et digitales.

M. le président Philippe Latombe. Je cède la parole aux orateurs de groupe.

M. Aurélien Saintoul (LFI-NFP). Je souhaite évoquer en premier lieu le rôle des agents assermentés par l'État qui auront pour fonction de mener des contrôles. Disposez-vous d'une forme de cahier des charges à ce titre ? Quel sera le cadre financier ? Qui sera le donneur d'ordre ?

Ma deuxième question concerne la saisine d'une commission des sanctions en cas de manquement ou d'infraction aux obligations contenues dans la directive

REC. Quel sera son statut ? Pourquoi devra-t-elle être rattachée directement au premier ministre ? Constitue-t-elle une juridiction de première instance ? Si ces sanctions sont d'ordre administratif, quelle sera la voie de recours ?

Enfin, la commission des sanctions ne peut sanctionner que les personnes privées. Pourtant, la directive n'établit pas de différence entre les OIV, qu'elles soient privées ou publiques. J'aimerais donc connaître la logique qui prévaut pour cette distinction.

M. Sébastien Saint-Pasteur (SOC). Sous la présidence Pompidou, un document pionnier, rédigé à la demande du secrétariat à la défense américain, identifiait déjà les vulnérabilités des systèmes d'information, notamment les risques d'accès non autorisé, de divulgation accidentelle ou d'infiltration délibérée.

Plus de cinquante ans plus tard, l'ombre portée par les menaces cyber a grandi de manière exponentielle. Fort de ce constat que nous partageons tous, je souhaite m'attarder sur plusieurs points. Je pense d'abord à la définition et au respect du périmètre des entités concernées, qui diffère des nomenclatures de l'Anssi auxquelles nous sommes habitués. Ensuite, comment les contrôles pourront-ils être réalisés quand on pense que dans la plus vaste région de France, la région Nouvelle Aquitaine, il existe seulement deux délégués régionaux de l'Anssi pour douze départements ?

Je m'interroge également sur les entités qui ne sont pas concernées. Une commune de moins de 3 000 habitants appartient probablement une intercommunalité à laquelle elle est reliée par des systèmes informatiques intégrés ou un établissement médico-social, qui traitera des données de santé sensibles. Le flou demeure donc pour les principaux intéressés. Qui plus est, le groupement d'intérêt public « Action contre la cybermalveillance » est aujourd'hui largement sous-doté pour faire face à ces défis. Un récent rapport sénatorial a pointé que les cyberattaques représentaient près de 90 milliards d'euros d'impact pour l'économie française.

Dès lors, comment garantir une transposition lisible pour l'ensemble des acteurs, même les plus petits ? Comment comptez-vous conseiller le gouvernement afin que les moyens d'accompagnement soient bien au rendez-vous, au plus près du terrain ?

Mme Laetitia Saint-Paul (HOR). Au sein du groupe Horizons, nous sommes sensibles à votre volonté d'associer les parlementaires à la RNS. Cependant, sur certains sujets, je suis restée sur ma faim. À titre d'exemple, dans la RNS 2022, l'intelligence artificielle (IA) n'est mentionnée que deux fois.

Je me permets de vous faire part de deux sujets que je souhaiterais voir figurer dans la prochaine RNS. Tout d'abord, la question du *lawfare* ou de la guerre juridique s'applique parfaitement à la confrontation dans les espaces communs, notamment cyber. Ensuite, la configuration du secrétariat général de l'armement nous permet-elle d'être agile sur les enjeux de haute technologie, de start-up, à

l'instar du modèle américain de la *Defense Advanced Research Projects Agency* (Darpa) ? De manière générale, notre modèle de travail interministériel est-il suffisamment agile pour faire face à l'hybridité de la conflictualité dans les espaces communs ? Enfin, s'agissant de la loi qui nous concerne, quelles en sont principales lacunes ?

M. Nicolas Roche. Monsieur Saintoul, les agents assermentés seront les mêmes qu'aujourd'hui. Le dispositif d'assermentation ne changera donc pas de manière radicale.

Ensuite, la commission des sanctions ne relève pas d'une autorité juridictionnelle en tant que telle. En revanche, comme toute mesure de police administrative, ces décisions seront susceptibles de faire l'objet de recours en excès de pouvoir devant la juridiction administrative et jusqu'au Conseil d'État.

La distinction entre acteurs privés et publics concerne la non-application des sanctions administratives aux collectivités territoriales. Cet élément tient au fait qu'*in fine*, le délégataire porte l'obligation qui lui est faite de contribuer à la sécurité nationale et à la résilience de la nation.

Les travaux préparatoires au projet de loi n'ont pas convaincu ses auteurs qu'il serait pertinent d'infliger des sanctions à des collectivités territoriales pour des manquements de leurs délégataires de service public, dans les cas d'activités d'OIV et en particulier parce que des sanctions pécuniaires sont ensuite définies en fonction d'un chiffre d'affaires. Le choix a donc été établi à ce stade de ne pas intégrer les collectivités et les acteurs publics des collectivités territoriales dans le champ des mesures qui auparavant relevaient de mesures pénales. À ce titre, le passage d'un régime de sanctions pénales à celui de sanctions administratives m'apparaît constituer une bonne méthode.

Monsieur Saint-Pasteur, il n'existe pas de critère de population pour des opérateurs ou des activités d'importance vitale des collectivités territoriales et des activités d'importance publique dans le titre I^er^.

Le directeur général de l'Anssi vous a exposé la semaine dernière le passage d'une logique de pilotage très précis par l'Anssi des OIV dans le domaine cyber à l'ensemble de la mise en œuvre de la directive NIS 2. Il vaut mieux prévenir que guérir ; en conséquence, l'accompagnement de l'ensemble des collectivités dans la mise en œuvre de la partie cyber de NIS 2 constitue un élément essentiel.

Madame Saint-Paul, j'ai pris bonne note des sujets que vous jugez prioritaires. Je peux vous rassurer en partie : nous conduirons ces travaux avec les parlementaires de la commission de la défense lors des semaines à venir. Les sujets que vous avez évoqués ont été pris en compte dans la RNS, même si j'ignore s'ils le seront à la mesure de ce que vous souhaitez. Ces travaux seront ensuite poursuivis par des consultations avec la représentation nationale, puis des validations par les autorités politiques, qui devraient intervenir d'ici la fin du mois.

M. le président Philippe Latombe. Comment pouvons-nous intégrer ce texte dans le cadre d'une construction d'une autonomie stratégique de cybersécurité, une forme de « BITC », sur le modèle de la BITD ?

M. Nicolas Roche. Ces sujets sont très bien identifiés dans la stratégie nationale cyber et par notre impératif de souveraineté numérique. Dans le cadre des travaux de la RNS, nous avons identifié un certain nombre d'enjeux et de défis pour la BITD. La structuration de la BITD française, son pilotage, son suivi, la relation entre les services de l'État et les acteurs privés me semblent d'une bonne qualité.

L'enjeu consiste aujourd'hui à reproduire ce dispositif pour la base industrielle et technologique de sécurité nationale (BITS), dont les questions cyber et numériques sont parties intégrantes. À ce titre, l'État doit mener un effort de structuration de sa réflexion sur cette BITS, notamment pour identifier des priorités, les sujets technologiques et les acteurs privés essentiels à notre souveraineté. Cette action a commencé dans le cadre de la RNS, mais devra faire l'objet de travaux complémentaires.

M. le président Philippe Latombe. Je vous remercie.

3. Table ronde réunissant des associations d'élus, jeudi 15 mai 2025 à 9 heures 30

Lors de sa réunion du jeudi 15 mai 2025, la commission spéciale a organisé une table ronde d'associations d'élus, avec la participation de M. Michel Sauvade, co-président de la commission numérique nationale (AMF) ; Mme Constance Nebbula, vice-présidente de la Région Pays de la Loire en charge du numérique et de l'intelligence artificielle et M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique (Régions de France) ; Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique à Intercommunalités de France.

M. le président Philippe Latombe. Mes chers collègues, nous reprenons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde consacrée à un sujet central : la cybersécurité des collectivités territoriales.

Nous avons souhaité entendre les représentants des différents niveaux de collectivités pour plusieurs raisons. La première tient à la vulnérabilité numérique de nos services publics locaux. La troisième étude 2024 de Cybermalveillance.gouv.fr sur la maturité cyber des collectivités de moins de 25 000 habitants montre qu'une collectivité sur dix déclare avoir été victime d'une ou plusieurs attaques au cours de l'année dernière, l'hameçonnage étant la cause principale dans 30 % des cas. Les conséquences pour les collectivités sont lourdes : interruption de service, destruction, vol de données, pertes financières.

Mais ce sont les usagers qui en subissent les effets : suspension des inscriptions ou des paiements en ligne pour la cantine scolaire, retard dans le versement d'allocations par les centres d'action sociale. En dépit de ces éléments, l'étude montre que 44 % des communes touchées se considèrent faiblement exposées au risque et que 18 % ne savent pas comment évaluer leur niveau d'exposition. Dans ce contexte, votre retour d'expérience nous est particulièrement précieux pour déterminer quel niveau d'obligation inscrire dans la loi et où placer le curseur.

La seconde raison de cette table ronde est liée à l'objet même du texte que nous examinons. Ce projet de loi vise à renforcer la cybersécurité des collectivités dans le cadre de la transposition de la directive européenne NIS 2 (*Network and Information Security 2*), qui établit un niveau commun de cybersécurité dans toute l'Union européenne (UE).

L'article 8 du projet de loi qualifie d'entités essentielles les régions, les départements, les communes de plus 30 000 habitants, ainsi que leurs établissements publics administratifs (EPA) lorsqu'ils exercent des activités relevant de secteurs hautement critiques ou critiques, les communautés urbaines, les communautés d'agglomération comprenant au moins une commune de plus de 30 000 habitants et les métropoles, leurs EPA, lorsqu'ils exercent des activités relevant de secteurs hautement critiques ou critiques. L'article 9 qualifie d'entités importantes les communautés d'agglomération ne comprenant pas au moins une commune de plus de 30 000 habitants, les communautés de communes et leurs EPA dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques.

L'article 14 du projet de loi prévoit que les entités qui ont été qualifiées d'essentielles ou d'importantes doivent mettre en œuvre un certain nombre de mesures techniques, opérationnelles et organisationnelles, pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent, ainsi que pour éliminer – ou à tout le moins réduire – les conséquences que les incidents engendrent sur les destinataires de leurs services.

Nous avons le plaisir d'accueillir aujourd'hui M. Michel Sauvade, vice-président du conseil départemental du Puy-de-Dôme, maire de Marsac-en-Livradois, qui représente l'association des maires de France et des présidents d'intercommunalités (AMF) ; Mme Constance Nebbula, vice-présidente de la région Pays de la Loire en charge du numérique et de l'intelligence artificielle et M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique, représentant l'association Régions de France ; ainsi que Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique à Intercommunalités de France, par ailleurs vice-présidente déléguée à l'économie numérique et aux systèmes d'information et à la culture de la communauté des communes de Lacq-Orthez. Elle s'exprimera également au nom de France urbaine.

Mesdames, messieurs, nous serons particulièrement attentifs aux points du texte qui vous paraissent poser difficulté, ainsi qu'à vos propositions concrètes pour en améliorer la mise en œuvre dans les collectivités.

M. Michel Sauvade, coprésident de la commission numérique nationale de l'Association des maires de France. Comme vous l'avez rappelé, les collectivités sont souvent en première ligne face à ces attaques, à telle enseigne que l'AMF y a consacré plusieurs ateliers dans le cadre de son congrès. Notre commission numérique se préoccupe régulièrement de ces sujets en partenariat avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) et les services de l'État concernés.

Nous partageons l'ambition d'un renforcement de la cybersécurité pour les communes et les établissements publics de coopération intercommunale (EPCI), mais sommes très inquiets sur le contenu du projet de loi concernant les conditions dans lesquelles ces collectivités et EPCI devront mettre en œuvre les obligations. En effet, ces nouvelles obligations imposées par le projet de loi entraîneront des charges supplémentaires importantes pour les communes et les intercommunalités. J'ajoute qu'aucune étude d'impact n'a pu proposer jusqu'à aujourd'hui d'évaluation chiffrée de ces conséquences sur le plan financier et des ressources humaines.

Il existe simultanément une sorte d'injonction contradictoire de la part du gouvernement – du moins dans ses déclarations – et de la Cour des comptes, qui contestent l'augmentation des dépenses de fonctionnement du bloc communal. Quel que soit le caractère légitime de l'intention, cette injonction contradictoire pose problème.

Ensuite, compte tenu de la disparité des collectivités, nous regrettons que la loi ne puisse inscrire une progressivité qui permettrait justement de lisser ou d'atténuer les tensions attendues sur la filière des métiers cyber et les contraintes budgétaires que nous connaissons dans nos collectivités. Dans ce contexte, pour l'AMF, la transposition de la directive NIS 2 ne doit pas ignorer cette réalité et doit s'inscrire dans une logique de transition progressive et d'un accompagnement très marqué de l'État. Parallèlement, l'AMF demande que le périmètre des collectivités soumises à NIS 2 soit plus restreint, notamment pour les communautés d'agglomération et de communes.

Lors de la discussion au Sénat, des avancées ont été obtenues concernant justement le périmètre d'application pour les communautés d'agglomération, et l'AMF souhaite que, dans le cadre de la discussion à l'Assemblée nationale, le périmètre d'application pour les communautés de communes soit également revu. Pour mémoire, l'AMF avait adressé un courrier au premier ministre le 7 mars dernier pour l'alerter justement sur cette situation des communautés d'agglomération et des communautés de communes.

Les propositions de l'AMF dans le cadre de ce projet de loi concernent seulement la directive NIS 2 et sont relatives aux mesures destinées à assurer un

niveau élevé commun de cybersécurité dans l'ensemble de l'Union. Le périmètre des entités essentielles retenu par le gouvernement pour les communes et les EPCI a évolué depuis la discussion au Sénat. Il résulte, nous semble-t-il, d'un choix du gouvernement qui peut être analysé comme une surtransposition de la directive.

Par ailleurs, l'AMF s'interroge sur le périmètre réel des communes concernées. Il n'est pas clair, notamment du fait des rapports étroits entre les communes et leurs EPCI, et de l'imbrication extrêmement variée des services informatiques et des mutualisations de personnel. Le référentiel de cybersécurité nous interroge également, puisqu'il dressera un tableau des prescriptions, réparties en une vingtaine d'objectifs applicables aux entités essentielles ou aux entités importantes, les obligations pour les entités essentielles étant plus contraignantes. Ces objectifs seront précisés ultérieurement dans un décret en Conseil d'État. En conséquence, le maire ou le président de l'EPCI sera *in fine* responsable de la sécurité numérique et du suivi de la conformité des systèmes d'information réglementés aux mesures édictées dans le référentiel de sécurité.

Quelles sont nos propositions ? L'AMF est soucieuse de la question de la cybersécurité et souhaite que l'application de cette directive soit un succès effectif. Toutefois, il faut que le législateur tienne compte de la réalité des moyens des communes et EPCI, afin que la mise en œuvre puisse être supportable financièrement, faisable techniquement et qu'elle soit progressive. Nous tenons donc vraiment à vous alerter sur la contradiction de ce texte avec les observations du gouvernement et de la Cour des comptes sur la maîtrise attendue de nos dépenses. De plus, il est difficile de concilier l'efficacité numérique et le maintien en l'état de nos systèmes d'information (SI).

Des consultations ont bien été conduites par l'Anssi, mais les préoccupations qui ont été exprimées par les associations d'élus n'ont pas reçu de réel écho à l'échelon politique, bien que l'AMF ait particulièrement insisté sur l'absence d'étude d'impact financier des nouvelles obligations, les nouvelles charges induites par les nouvelles obligations, l'absence de progressivité dans la mise en œuvre de la loi, le risque réel des tensions sur les métiers cyber et l'absence de visibilité sur un éventuel accompagnement de l'État.

L'adoption de la loi par le Sénat le 12 mars dernier a permis des avancées et l'AMF s'est félicitée de l'évolution concernant le périmètre de la loi pour les communautés d'agglomération. En revanche, toutes les communautés de communes sont restées assujetties au statut d'entités importantes, ce qui nous pose problème.

Les autres dispositions votées par le Sénat qu'il conviendrait de conserver concernent l'accompagnement de l'État. Le projet de loi prévoit que l'État élabore une stratégie nationale en matière de cybersécurité, comprenant notamment les modalités de soutien aux collectivités territoriales et leurs groupements. Concernant le règlement de sécurité, le décret en Conseil d'État qui déterminera les conditions d'élaboration de modifications éventuelles et de publication du référentiel

s'appliquant aux entités essentielles et importantes devra être adapté à leur degré d'exposition aux risques, à leur taille, à la probabilité de survenance d'incidents et leur gravité, en prenant en compte également les conséquences économiques et sociales de telles attaques. Ce règlement de sécurité devra également définir les modalités de concertation des représentants des entités concernées et des associations d'élus.

Concernant plus particulièrement la discussion à venir à l'Assemblée nationale, l'AMF demeure mobilisée. Nous souhaitons toujours que le périmètre d'application de la loi aux communautés de communes soit restreint. Je pense ici au non-assujettissement des communautés de communes inférieures à 30 000 habitants à NIS 2. En effet, nous sommes persuadés que la mise en œuvre sera pour le moins particulièrement difficile. Dans cette hypothèse, sur les 990 communautés de communes, seules 211 seraient assujetties au statut d'entité importante.

Parallèlement, il s'agit également de laisser le temps nécessaire à ces collectivités pour mettre en place de nouvelles règles de cybersécurité, lesquelles doivent être adaptées à leur réalité. Cette mesure a également pour objectif de ne pas créer une pression supplémentaire dans la mise en œuvre des règles de cybersécurité, alors que le marché est déjà sous tension.

Les communautés de communes entreront dans ce marché en même temps que de très nombreuses entreprises. Pour autant, il est utile d'assurer l'information et la formation des élus et des agents, ainsi que de promouvoir la diffusion des bonnes pratiques dans ces collectivités, comme dans les communes. À ce titre, je rappelle l'action de l'AMF pour sensibiliser les communes les plus petites, en partenariat avec les services de gendarmerie. Nous souhaitons que ces enjeux soient finalement inclus dans le projet de loi, en intégrant ce soutien, les programmes d'action de l'État et de ses opérateurs. L'AMF souhaite enfin une mise en œuvre progressive de la loi pour les communes et les EPCI assujetties à NIS 2 en métropole et dans les outre-mer.

Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique à Intercommunalités de France. À l'heure de la numérisation globalisée des services, du développement de la data, de l'intelligence artificielle (IA), des villes intelligentes et de la vidéosurveillance, la surface des attaques augmente de manière exponentielle pour tout le monde, y compris les collectivités. Ainsi, nous avons dénombré 187 attaques entre 2022 et 2023, mais ce chiffre tend à augmenter.

Nos associations Intercommunalités de France et France urbaine ont accueilli avec bienveillance la proposition de l'Anssi d'intégrer dans le dispositif NIS 2 l'ensemble des entités que nous représentons, aussi petites ou aussi grandes soient-elles. Nous saluons d'ailleurs l'écoute de l'Agence lors des diverses consultations. Nous positionnons l'intercommunalité comme l'espace de mutualisation et bassin de vie par excellence pour faire rempart.

En effet, Intercommunalités de France joue déjà un rôle majeur de cybersécurité en mutualisant les moyens humains, financiers et techniques pour protéger l'ensemble de ses communes membres face à un risque numérique grandissant. Avec la directive NIS 2, l'association deviendra un acteur clé pour accompagner les communes, notamment les plus petites d'entre elles, dans la mise en conformité avec les nouvelles obligations.

Grâce à cette approche collective et solidaire territoriale, les intercommunalités renforcent la résilience numérique des territoires, garantissant une meilleure protection contre les cyberattaques et une gestion plus efficace des ressources en cybersécurité. Depuis la réalisation de notre baromètre de maturité numérique des collectivités en 2023, nous avons pu constater que sept intercommunalités sur dix ont au moins mis en œuvre des actions de sensibilisation et de formation auprès des agents et des élus. Aujourd'hui, une attaque peut concerner une petite commune de 200 habitants, mais entraîner des répercussions sur le système d'information de l'intercommunalité dont elle est membre. Il nous semble donc important d'intégrer tout le monde dans un dispositif, certes très lourd. Mais si nous le faisons de manière intelligente, cela fournira l'occasion de nous structurer dans ce domaine, puisque la cybersécurité et la cyberdéfense seront de toute façon notre quotidien.

Si nous accueillons avec bienveillance cette transposition à l'ensemble des collectivités que nous représentons, nous restons lucides. Nous sommes conscients des écueils qui pourraient empêcher l'effectivité de cette loi. Nous partageons effectivement les inquiétudes et les difficultés mentionnées par M. Sauvade. Dans un premier temps, nous exprimons un besoin de portage politique et de coordination ministérielle.

Nous avons pris connaissance des annonces récentes en termes de sensibilisation des 15 000 entités essentielles et importantes, dont les 1 500 collectivités qui devront s'enregistrer auprès de l'Anssi, mais nous avons peu de détails sur la manière dont cela se déroulera, ni sur l'accompagnement qui est attendu.

Par ailleurs, il est aussi parfois difficile pour les associations d'élus de traiter efficacement des sujets du numérique avec le gouvernement, car la coordination interministérielle est peu lisible. Par ailleurs, par l'intermédiaire des Interconnectés, nos deux associations d'élus ont lancé un groupe de travail dédié à l'élaboration de la phase réglementaire. Ce groupe miroir est composé de quinze collectivités allant de la communauté de communes à la métropole. Ce collectif a été réuni trois fois et a déjà pu analyser les impacts des objectifs de sécurité exprimés par la partie réglementaire.

Nous avons reçu les vingt objectifs de sécurité qui devront être traités et mis en œuvre. Ces objectifs de sécurité seront ensuite détaillés en sous-objectifs. Nous allons également échanger sur les leviers d'action et proposer des solutions à la future réglementation. Ce collectif a naturellement relevé des écueils importants,

notamment en matière de compétences, de ressources humaines manquantes et d'obligations qui nous incombent d'après la réglementation, mais que nous serons dans l'incapacité de tenir. Les besoins concrets ont été regroupés dans un compte rendu qui sera remis à l'Anssi très prochainement. Après la validation de l'Anssi, nous serons en mesure de vous fournir ce document, si vous le souhaitez. Celui-ci explique l'ensemble de la démarche et ce que nous prévoyons de faire pour accompagner nos collectivités.

Je souhaite que nous puissions également parler de deux initiatives des Interconnectés qui sont étroitement associés à cette thématique : le groupe de travail « Petits territoires » et le projet « TIE Break » (Trajectoire d'indépendance européenne numérique). Ce dernier extraira l'ensemble des outils utilisés par nos collectivités (logiciels, outils de cyber, outils métiers), afin que l'Anssi les évalue et nous fournisse des préconisations.

En conclusion. rien ne sera possible sans un accompagnement technique et financier structuré. Un parcours cyber doté d'un audit précis a été proposé par France Relance, incluant un plan d'accompagnement pour améliorer la sécurité. Mais il n'a bénéficié qu'aux plus grosses entités, soit 78 communautés de communes sur 992. Il sera possible d'imaginer par la suite un « parcours NIS 2 », qui pourra être adapté en fonction des entités, au-delà d'un accompagnement purement financier. Enfin, un travail coordonné de toutes nos instances et structures sera nécessaire, quelle que soit leur nature.

M. le président Philippe Latombe. Nous sommes contraints par le temps lors de nos travaux. Pourriez-vous nous transmettre le document même s'il n'a pas été entièrement validé par l'Anssi ? Notre rapporteur pourrait ensuite échanger sur cette base avec l'Anssi. L'examen du texte devrait avoir lieu début juillet ou début septembre.

Mme Marlène Le Dieu De Ville. C'est entendu.

Mme Constance Nebbula, vice-présidente de la région Pays de la Loire en charge du numérique et de l'intelligence artificielle à Régions de France. Notre intervention s'effectuera à deux voix, puisque j'interviendrai en compagnie de M. Ventadour. Il s'agit pour nous de porter la parole des régions, qui sont extrêmement concernées par les directives aujourd'hui abordées, notamment parce que ces régions sont définies comme des entités essentielles. Notre objectif consiste à ce titre à vous indiquer les points bloquants, les risques techniques, financiers et organisationnels exprimés par les régions. Dans un premier temps, nous évoquerons le sujet cyber dans sa globalité, et notamment le périmètre qui pourrait être octroyé ou laissé aux régions. Dans un second temps, nous insisterons sur le lien avec l'Anssi, notamment sur le sujet des financements.

M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique à Régions de France. En préambule, je tiens à saluer la démarche de concertation engagée par votre

commission. Je vous parle depuis la Martinique qui, il y a près de deux ans, a souffert d'une cyberattaque ayant mis à mal toute l'organisation de la collectivité territoriale.

Des préoccupations majeures se font jour de la part de l'ensemble des collectivités, dont les régions. La première concerne l'accompagnement de ces collectivités. Les régions sont ainsi désignées comme des entités essentielles. Le texte prévoit un délai de trois ans pour se mettre en conformité, mais en ne précisant pas assez les moyens qui seront associés, qu'il s'agisse des moyens humains ou financiers qui doivent être adaptés, notamment s'agissant des CSIRT (*Computer Security Incident Response Team*). Ce délai de trois ans risque donc de ne pas suffire, tant les obligations prévues sont lourdes (cartographie, audits, plans de sécurisation, suivi des incidences et gouvernance). Certaines régions font face à des réalités complexes.

D'autres territoires, comme la Martinique et la Réunion, ont également souffert de sévères attaques. Plus largement, les outre-mer ne disposent pas forcément des ressources en interne. Lorsque la Martinique a subi cette cyberattaque, je me souviens avec émotion avoir vu débarquer une équipe d'une douzaine de techniciens – notamment de l'Anssi – pour venir à notre secours, mais ils n'ont pas pu rester pendant toute la durée du sinistre. Nous avons donc été contraints de fonctionner ensuite à distance. Cet exemple montre bien que les territoires éloignés ne sont pas forcément armés pour résister à de telles attaques.

Le projet de loi introduit dans son article 5 *bis* la notion de stratégie nationale de cybersécurité, pilotée par le premier ministre. Nous nous en félicitons et demandons que cette stratégie prévoie explicitement les modalités de soutien opérationnel et budgétaire aux collectivités, par exemple en lien avec les objectifs et les financements de France 2030.

Deuxièmement, aucune étude d'impact n'a été véritablement menée sur les coûts engendrés pour les collectivités. La ministre en charge du numérique a reconnu en audition que les collectivités devraient consacrer jusqu'à 10 % de leur budget informatique à la cybersécurité. Pour certaines régions, notamment les plus importantes, cela représenterait plusieurs millions d'euros par an, sans compter les audits et formations préalables ou le remplacement des infrastructures obsolètes. En outre, NIS 2 ne concerne pas uniquement les opérateurs publics et les agents, mais également les partenaires et prestataires avec lesquels nous allons devoir travailler, qui devront être labellisés. Or, dans certaines régions, ces partenaires n'ont pas forcément les moyens de monter en puissance ; il sera nécessaire de les accompagner. Nous demandons donc que l'État commande une étude de coût exhaustive, afin de financer réellement la montée en puissance exigée par NIS 2.

Troisièmement, il convient d'évoquer le périmètre d'action. Lors de nos discussions au sein de Régions de France, a été relevé un point d'attention concernant les lycées. En effet, ces établissements relèvent des régions. Le projet de loi ne précise pas si les infrastructures informatiques des lycées rentrent dans le

périmètre de responsabilité des régions au titre de la directive. Or il peut s'agir parfois de dizaines de milliers de postes informatiques, dont les niveaux de sécurisation sont très hétérogènes. En conséquence, nous demandons une clarification explicite dans les décrets d'application, afin d'éviter un vide juridique ou une responsabilité mal encadrée.

Les régions ne contestent pas le projet de loi, qu'elles appellent au contraire de leurs vœux. Pour autant, sa mise en œuvre doit être pragmatique, équitable et accompagnée. Nous attendons que l'État, aux côtés des régions, mais plus largement des collectivités, joue également un rôle d'accompagnateur et de financeur.

Mme Constance Nebbula. J'insisterai pour ma part sur la relation avec l'Anssi telle qu'elle est envisagée dans le projet. Je pense notamment à la création des organismes relais agréés par l'Anssi prévus à l'article 24 du projet de loi. Il est ainsi indiqué que l'Anssi peut agréer des organismes publics ou privés, en tant que relais dans la prévention et la gestion des risques cyber.

Il apparaît intéressant de considérer que les CSIRT et les dynamiques autour des campus cyber des régions sont naturellement pressentis pour assurer ce rôle d'organisme-relais agréé par l'Anssi dans les territoires. Ces éléments conduisent à soulever un certain nombre de questions. Quels seront les moyens financiers alloués par l'État aux régions pour leur permettre de faire vivre ces structures ? Serait-il possible de développer une forme de labellisation NIS 2 pour attester de la conformité des entités qui sont concernées par le champ d'application de la loi « Résilience et cybersécurité », notamment pour permettre à ces entités de justifier plus simplement de leur conformité à la directive en cas de contrôle ?

Il s'agirait donc de faciliter la conformité des entités régulées, mais pour permettre de développer une offre complémentaire pour les CSIRT. Cette valeur ajoutée offrirait la possibilité d'équilibrer un modèle financier qui n'est pas trouvé aujourd'hui. S'agissant de cette question de labellisation, il serait opportun que la ministre du numérique confie à l'Anssi la mission de définir un label de conformité, afin que les entités puissent s'en prévaloir. L'Anssi prendrait donc le contrôle de l'agrément et aurait accès à un label valorisant l'engagement des CSIRT, notamment en région, pour pérenniser leurs actions.

Nous demandons également la prolongation du financement. Régions de France a d'ailleurs adressé un courrier au premier ministre il y a quelques semaines à ce sujet. Bien entendu, les régions ne sont pas surprises de l'arrêt du financement. En revanche, une dynamique cyber nationale avait été amorcée avec le lancement des CSIRT, qui va malheureusement s'interrompre, laissant le relais aux régions. Cet aspect pose nécessairement question. Pour rappel, l'Anssi avait consacré 1 million d'euros à cette initiative sur une période de trois ans, qui arrive aujourd'hui à son terme. Nous opérons donc en mode « débrouille » pour continuer à faire vivre ces CSIRT, en l'absence du soutien de l'État.

Au-delà du financement, des nouveaux acteurs sont apparus dans la chaîne, notamment le 17Cyber, plateforme portée par Cybermalveillance.gouv.fr. De leur côté, les CSIRT sont organisés autour de centres d'appels traités par des opérateurs issus des partenaires et prestataires connus, labellisés, sécurisés, en région et en proximité. Il s'agit donc de trouver le bon partenariat entre ces différents outils, ce qui n'est pas forcément évident, compte tenu de la différence de points de vue entre Cybermalveillance.gouv.fr et les régions.

Régions de France demande que l'État participe au financement et à la pérennité des CSIRT par l'intermédiaire de l'Anssi et clarifie les rôles de Cybermalveillance.gouv.fr et de l'Anssi, au-delà de la simple signature de partenariats, lesquels sont très différents d'une région à l'autre. À ce titre, nous déplorons un certain manque d'uniformité et de vision nationale.

En conclusion, les régions sont vraiment vigilantes concernant la préparation des décrets d'application, notamment le décret relatif à l'élaboration du référentiel d'exigences techniques et opérationnelles. Par ailleurs, les régions n'ont pas attendu les discussions du moment pour anticiper et travailler sur le risque cyber. Néanmoins, nous souhaiterions être accompagnés, soutenus, dans le cadre d'une dynamique nationale.

M. Éric Bothorel, rapporteur général. Nous sommes tous convaincus que les moyens financiers qu'il sera nécessaire de réunir, fussent-ils soutenus par l'État, ne sont pas commandés par NIS 2, mais par l'état de la menace et de l'activité cybercriminelle. De fait, l'Anssi a dû traiter 218 incidents cyber concernant les collectivités, dont 144 ayant trait aux communes, soit une moyenne de dix-huit par mois. Nous portons donc une responsabilité collective, afin de mettre en œuvre des éléments nous permettant de faire face à cette activité cybercriminelle. Pour reprendre les mots de Vincent Strubel, nous avons tous découvert qu'il n'est pas nécessaire d'être une cible pour être une victime. Les collectivités continuent de l'apprendre à leurs dépens. Il conviendra évidemment, au travers de ce texte, qui s'inscrit dans une doctrine européenne, de trouver les organisations qui nous permettent d'être plus résistants, plus résilients et plus efficaces.

Ma collègue Anne Le Hénanff est rapporteure de la partie du projet de loi relative à NIS 2. Étant retenue en circonscription, elle m'a transmis ses questions, que je m'apprête à vous poser, tout en partageant ses préoccupations. Quel est votre avis sur les ajouts et modifications apportés par le Sénat concernant les collectivités territoriales ? Jugez-vous le seuil des 30 000 habitants pertinent et adapté ? À défaut, quel seuil privilégieriez-vous ? Pour ma part, je suis surpris que le Sénat n'ait pas traité de manière identique les communautés d'agglomérations et les communautés de communes.

Quel est votre avis sur les critères retenus par la Belgique pour déterminer si une collectivité était assujettie ou non aux dispositions de la directive NIS 2 ? Avez-vous évoqué avec l'Anssi le cas des communes dites touristiques dont la population permanente est inférieure à 30 000 habitants mais pouvant aisément

dépasser ce seuil en période estivale ? Compte tenu des services publics dont elles disposent, pensez-vous qu'elles devraient être assujetties à NIS 2 ? Enfin, quel est le retour des collectivités concernant la solution des CSIRT régionaux ? Les sollicitent-elles ? De quelle manière ? Quelle est en pratique l'aide apportée ? Est-elle optimale ? D'après vous, les CSIRT doivent-ils jouer un rôle dans la mise en œuvre de NIS 2 ?

Madame Nebbula, je ne suis pas opposé à l'idée d'un modèle différent pour les CSIRT. Le président de ma région est ainsi très attaché à l'expérimentation et à la différenciation. Le fait que les campus cyber et les CSIRT reposent sur les modèles différents ne fait pas obstacle à une bonne coordination entre eux pour une meilleure efficacité dans un dispositif plus global.

Mme Constance Nebbula. Tout d'abord, je vous remercie de prendre le temps de conduire cette concertation. Nous avions d'ailleurs eu l'occasion de l'indiquer au Sénat au début du mois de février, tant ces occasions sont rares. Nous profitons de NIS 2 pour évoquer ces sujets, pour parler de stratégie, de politique cyber, mais aussi des financements, des moyens, de l'organisation. C'est peut-être un peu tardif ; néanmoins, mieux vaut tard que jamais.

Lors de la discussion au Sénat, Régions de France a rappelé son attachement à une vraie stratégie de l'État en matière de cybersécurité. La nouvelle rédaction du projet de loi comprend de fait « l'élaboration » par le premier ministre d'une stratégie nationale en matière de cybersécurité, inscrite dans le nouvel article 5 *bis*, qui détaille les modalités de soutien aux collectivités territoriales et à leurs groupements. Il y a là deux signaux très intéressants, qu'il faut pérenniser : une véritable ambition politique stratégique en matière de cybersécurité ; et la définition des modalités de soutien aux collectivités territoriales et à leurs groupements. Nous considérons que ces éléments vont dans le bon sens et qu'ils doivent être pérennisés.

La deuxième question concernant Régions de France porte plus sur les CSIRT. Lorsque nous indiquons que chacun dispose de modèles différents, il ne s'agit pas d'une critique. Simplement, les solutions à nous apporter ne sont peut-être pas identiques pour tout le monde. Par exemple, il n'existe pas de CSIRT en Martinique ; certaines régions possèdent des campus cyber, d'autres non ; ailleurs, les CSIRT sont parfois intégrés à des campus cyber. À l'occasion de la concertation conduite avec nos collègues, nous avons été unanimes pour témoigner de notre volonté de bénéficier d'un accompagnement, au-delà d'un soutien financier. Nous sommes tous élus locaux et savons bien que le contexte budgétaire est compliqué.

Néanmoins, j'insiste pour signifier que nous évoluons tous aujourd'hui dans un mode « débrouille ». L'Anssi nous a aidés à effectuer l'amorçage, mais encore faut-il désormais trouver le modèle, les ressources humaines et les partenaires. À titre d'exemple, dans les Pays de la Loire, nous n'avions pas jusqu'à présent de structure juridique.

Il est donc nécessaire d'élaborer une vision nationale sur la manière dont les collectivités travailleront avec l'Anssi, mais également la répartition des rôles entre l'Agence, Cybermalveillance.gouv.fr, la gendarmerie et les différents dispositifs. Les très petites entreprises (TPE) et les petites et moyennes entreprises (PME) font aujourd'hui face à un flot très important de possibilités.

Soit chaque région communique bien sur son outil régional, mais la communication nationale n'est pas optimale ; soit la situation est inverse. Des choix doivent donc être opérés. De notre côté, nous considérons que ce qui est porté localement a plus d'impact que ce qui est porté sur le plan national. Mais les deux démarches doivent se dérouler en bonne entente, préalablement à la signature d'un partenariat.

M. Alexandre Ventadour. Il est exact que la Martinique n'a pas de CSIRT. Au moment où il était question de les mettre en place, nous avons été frappés par la très grande cyberattaque dont je parlais précédemment, laquelle a laissé des traces, encore visibles aujourd'hui. La mise en place n'a pas eu lieu, faute de visibilité sur le financement après « l'expérimentation » de trois ans. Comme de nombreuses collectivités, les territoires ultramarins ont connu des actions initiées sur le plan national, qui étaient ensuite basculées sur le financement propre des régions.

Nous ne disposons pas de CSIRT, mais nous tâchons de répondre aux incidents. Quoi qu'il en soit, nous nous efforçons de revenir dans cette initiative importante, qui nous met en lien avec l'ensemble du territoire. Les CSIRT doivent à la fois coopérer entre elles, mais aussi avec l'entité étatique. Il ne s'agit pas uniquement de protéger nos collectivités, mais également de permettre aux PME et TPE avec lesquelles nous travaillons, notamment sur ces aspects informatiques, numériques et de cybersécurité, de pouvoir monter en compétence.

C'est la raison pour laquelle nous en appelons à une forme de labellisation qui pourra en outre contribuer à l'établissement d'un *business model*, en étant conscient que l'argent public se fait rare actuellement. Nous savons pertinemment qu'il n'est pas possible de tout régler avec un financement national. C'est la raison pour laquelle nous proposons des solutions alternatives – car dans les domaines régaliens comme la sécurité ou la santé, les activités ne peuvent pas dégager de profits – si nous ne voulons pas concurrencer les acteurs privés de nos territoires, qui ne profitent pas de leur côté de l'argent public.

En conclusion, une forme de modèle hybride de financement sur les CSIRT régionaux serait extrêmement intéressante et extrêmement efficace, notamment pour la proximité de l'action.

Mme Marlène Le Dieu De Ville. Le seuil de 30 000 habitants constitue un critère important dans la proposition initiale de l'Anssi. Comme cela a été relevé par la commission supérieure du numérique et des postes, ce critère n'est sans doute pas le plus pertinent. Initialement, lorsque cette proposition d'intégrer les intercommunalités dans NIS 2 a été formulée, il était également prévu que les

communautés de communes de plus de 30 000 habitants, soient considérées comme entités essentielles, les autres étant des entités importantes.

L'Anssi n'avait pas conscience de l'existence de communautés de communes de 80 000 habitants ; elle pensait qu'au-delà de 30 000 habitants, le format de la communauté d'agglomération s'imposait. Nous avons donc expliqué que cela n'était pas le cas, ce qui a permis de rectifier le tir. Nous avons également souligné qu'entre une communauté de communes de 5 000 habitants et une autre de 80 000 habitants, les disparités de moyens sont telles que les services informatiques sont structurés différemment. Ces disparités ont éclaté au grand jour lors des plans France Relance et des parcours cyber, puisque seules les plus importantes collectivités ont été accompagnées, ce qui est à la fois quelque peu aberrant, mais également logique.

Quels peuvent être les autres critères ? La commission supérieure du numérique et des postes avait proposé que l'Anssi décide en fonction des compétences critiques, voire très critiques, que chacune collectivité peut exercer. Par exemple, une ville balnéaire qui voit sa population passer de 10 000 habitants à 100 000 habitants l'été pourrait être intégrée à juste titre dans le dispositif.

En conséquence, nous avons également relevé de notre côté quelques incohérences. Le Sénat n'a pas imposé aux communes de transférer les compétences pour le secteur dit critique de l'eau et de l'assainissement, faisant naître des situations complexes. Certaines communautés de communes intégreront ainsi l'eau et l'assainissement dans leur périmètre, mais cela ne sera pas le cas pour toutes. Nous nous posons des questions, puisque les communes de moins de 30 000 habitants ne sont pas soumises à NIS 2.

En résumé, le critère du nombre d'habitants n'était pas le plus pertinent, mais il faut désormais s'en accommoder. En outre, des amendements ont pu voir le jour. Je salue à ce titre celui qui permet aux communautés d'agglomération qui n'ont pas de villes de plus de 30 000 habitants de sortir du périmètre « entité essentielle ».

S'agissant de la coordination régionale, nos groupes de travail ont souligné la nécessité d'un accompagnement plus proche et plus local. Nous avons besoin de savoir à qui nous nous adressons et qui peut nous accompagner. En Nouvelle-Aquitaine, le CSIRT est imbriqué dans le campus cyber ; les relations sont bonnes. Mon intercommunalité fait partie du campus cyber et le travail est intéressant. Cependant, nous aimerions aller plus loin, à travers une généralisation au niveau national.

Par ailleurs, nous souhaitons que l'Anssi assure une présence plus active au niveau régional, pour nous accompagner dans toutes nos démarches.

M. Michel Sauvade. Nos échanges témoignent de la vision partagée des associations d'élus. À l'AMF, la commission numérique est présidée par deux élus, l'un étant vice-président d'un département et l'autre vice-président d'un conseil régional. Il existe donc naturellement une coordination sur cet ensemble. La table

ronde de ce jour montre également l'absence de portage politique. En tant que parlementaires et élus locaux, nous avons une responsabilité dans l'absence de ce portage.

Lorsque nous échangeons avec les directeurs des systèmes d'information (DSI) ou les responsables sécurité des systèmes d'information (RSSI), ils nous reprochent de les placer en première ligne sans qu'ils ne disposent pour autant de visibilité, ni de soutien. À l'AMF, nous avons en effet organisé une rencontre avec des DSI, dont les conclusions ont été assez perturbantes. Nous parlons aujourd'hui de la transcription de la directive NIS 2, mais plus globalement, les communes sont aujourd'hui confrontées à un problème de ressources humaines, pour pouvoir trouver des spécialistes en mesure de gérer nos réseaux et d'administrer nos serveurs.

Les amendements sénatoriaux sont intéressants, mais le travail doit être poursuivi. Je partage également l'interrogation concernant ce seuil des 30 000 habitants. Dans un souci de lisibilité, ce seuil pourrait emporter une cohérence globale dans le dispositif.

Ensuite, dans les communes touristiques, des blocages peuvent intervenir, mais il ne s'agit pas de cyberattaques. Ce problème du blocage est ainsi lié à l'insuffisance des infrastructures. Nous sommes sollicités par les communes, notamment en termes de couverture numérique. Lorsque des phénomènes de saturation surviennent, le système se bloque, non pas par malveillance, mais en raison de l'inadaptation des moyens.

D'une manière plus générale, pour les législateurs que vous êtes, l'enjeu consistera dans les semaines à venir à faire vivre et évoluer un texte, afin qu'il s'adapte au plus près du terrain, dans l'échelle, la temporalité, mais aussi dans l'anticipation en matière de cybersécurité. Dans le cadre de NIS 2, il ne s'agit pas d'agir en curatif, mais bien d'être capable d'anticiper une attaque qui, de toute façon, se produira à un moment ou un autre.

M. Thomas Gassilloud (EPR). En tant qu'ancien « jeune élu », je confirme que nous partons effectivement de loin en matière cyber. Il n'en demeure pas moins que le numérique est capital dans nos collectivités et que nous devons collectivement renforcer notre cybersécurité.

Je souhaite également revenir sur la question du seuil. Je partage l'idée que le critère du nombre d'habitants n'est pas forcément le plus adéquat, compte tenu des modes de gestion et des compétences très différentes, mais il s'agit peut-être du moins mauvais. Je n'ai pas encore suffisamment étudié le texte pour me positionner sur la pertinence du seuil à 30 000 habitants, mais il m'apparaît nécessaire de faire confiance aux élus pour déterminer l'approche en matière de cyber dans leur collectivité, dans une logique de subsidiarité et de libre administration des collectivités territoriales.

Lorsque j'étais élu local, j'ai ainsi constaté que les directives imposées par le niveau national coûtaient cher et n'étaient pas toujours appropriées. Au-delà, nous devons tous être vigilants quant au maillage des collectivités : si l'on en impose toujours plus aux collectivités, nous risquons de fragiliser l'existence de collectivités de plus petite taille. Or nous sommes pourtant toujours contents de trouver nos maires de proximité lorsqu'il s'agit de traiter des situations de crise, telles une crise sanitaire ou une crise cyber. Par-delà la transposition de NIS 2, ce texte peut nous permettre collectivement de développer la culture du risque et la culture de défense dans nos collectivités, dans une logique d'efficacité.

Comment la déclinaison de NIS 2 peut-elle constituer l'occasion d'une approche plus globale pour prévenir les risques au sens large dans nos collectivités, en lien avec les dispositifs existants, les correspondants défense, la gendarmerie nationale, les plans communaux de sauvegarde, les réserves communales de sécurité civile ? Par ailleurs, je suppose que les collectivités sont également soumises à certaines dispositions de la directive REC puisqu'elles gèrent des services d'énergie, d'eau et de transport. Quels sont les impacts de cette directive pour les collectivités territoriales ?

M. Arnaud Saint-Martin (LFI-NFP). Je remercie les intervenants pour ces éléments de restitution, qui montrent à quel point il est nécessaire d'investir massivement pour assurer la sécurisation des infrastructures et systèmes de nos collectivités locales. Lorsque j'étais élu municipal et communautaire de Melun, j'ai suivi de très près une cyberattaque qui a déstabilisé brutalement et durablement les services informatiques du conseil départemental de la Seine-et-Marne. Celle-ci fut le ferment d'une prise de conscience essentielle.

Je souhaite évoquer la consolidation d'une culture partagée des risques cyber. Le projet France Relance, lancé en 2021, consistait à investir 250 millions d'euros pour rapprocher le numérique du quotidien des Français. Dans ce cadre, 4 000 conseillers numériques ont été recrutés sous la forme de contrats aidés sur tout le territoire, formés et financés par l'État. Or ce projet doit s'arrêter en 2027, alors même que l'ensemble des objectifs n'ont pas été atteints. Les premiers contrats des conseillers se sont arrêtés en 2023 ; la seconde vague de fin de contrats interviendra en 2025 et la troisième en 2027. Par ailleurs, 13 millions de Français sont éloignés du numérique. La situation ne s'est pas améliorée, voire s'est dégradée, avec l'explosion de l'intelligence artificielle et l'augmentation des menaces cyber.

Face à ce constat, il est évident que les conseillers numériques sont essentiels dans les collectivités. En complément de France Services, ils accompagnent les usagers les plus vulnérables et les plus éloignés du numérique dans leurs démarches en ligne. Un travail immense reste à accomplir à travers une politique massive d'éducation d'une grande partie de la population pour faire face aux diverses menaces cyber qui peuvent aussi toucher les particuliers.

Il est donc urgent de construire une politique nationale stable de la médiation numérique. Le plan France Relance, mis en place depuis 2021, a souffert d'un cruel manque de stabilité – contrats aidés, contrats courts, sous-traitance – et d'un manque de planification. Les conseillers numériques recrutés restent en moyenne moins d'un an et demi en poste, dont six mois qui servent à pleinement les former. Il est pourtant nécessaire que le rôle des conseillers numériques soit étendu en lien avec ce projet de loi, pour faire face aux menaces, accompagner les usagers les plus vulnérables. De tels chantiers justifieraient une prolongation du rôle de ces conseillers et le réarmement d'une politique publique de la médiation numérique interministérielle.

Pour assurer la résilience numérique et l'adaptation de l'ensemble de la population, quel dispositif vous semble le plus utile à soutenir sur un plan budgétaire ? Que préconisez-vous pour assurer une politique d'éducation populaire aux enjeux de cybersécurité ? Pensez-vous qu'il soit nécessaire de pérenniser les emplois de conseillers numériques dans le cadre de ce projet de loi ?

Mme Geneviève Darrieussecq (Dem). Je partage également l'idée que notre société a besoin de prendre en compte ces risques cyber. Nous travaillons longuement sur ces sujets dans le cadre de la commission de la défense et constatons que nous sommes très vulnérables, à tous les niveaux. Les grandes entreprises réussissent à organiser leur défense, mais les PME et TPE éprouvent plus de difficultés. Le même parallèle peut être établi entre grandes et petites collectivités, qui sont par ailleurs liées entre elles par des liens numériques, qui constituent autant de fragilités potentielles.

En conséquence, nous devons tous être protégés. Quelle est selon vous la bonne échelle pour la mise en place de moyens organisationnels sur le terrain ? Faut-il privilégier un grand campus régional, un échelon départemental ? Enfin, il ne faut pas distinguer les besoins des entreprises et ceux des collectivités. Nous sommes embarqués dans le même bateau et souvent interconnectés.

Mme Laetitia Saint-Paul (HOR). Lorsque la commission des affaires étrangères a auditionné le directeur de l'Anssi, il a indiqué que les hackers ou les rançongiciels mettent en œuvre des ciblages très intelligents. Plutôt que d'attaquer frontalement, ils passent par les portes dérobées ; par les sous-traitants pour les entreprises, par les entités secondaires, pour les collectivités. Dès lors, je rejoins également l'interrogation de mes collègues concernant le seuil des 30 000 habitants, puisque ces hackers emploient des méthodes de contournement.

Ensuite, nous sommes très attachés à nos départements et régions d'outre-mer. J'ai acquis la certitude que ces outre-mer représentent la cible principale des stratégies hybrides qui s'attaquent à notre pays. Nous avons pu le constater lors des manœuvres d'ingérence étrangère de l'Azerbaïdjan envers la Nouvelle-Calédonie. Les outre-mer constituent également une cible dans le cadre de la lutte pour les espaces communs à l'échelle mondiale – notamment l'espace maritime. Leur éloignement des structures de soutien métropolitaines les rend d'autant plus

vulnérables. Dès lors, ce projet de loi peut leur permettre d'améliorer leur cyberdéfense, qu'elle soit civile ou militaire. Je souhaite donc vous interroger à ce sujet.

Enfin, j'ai été interpellé par la remarque de Mme Le Dieu De Ville s'agissant des problèmes de communication interministérielle. J'espérais pour ma part que sous l'égide du secrétariat de la défense et de la sécurité nationale (SGDSN), l'interministériel fonctionnerait. Pouvez-vous détailler à quel point les dysfonctionnements interministériels que vous avez mentionnés sont problématiques ?

Mme Marlène Le Dieu De Ville. Pour ma part, je fais partie d'un groupe de travail sur la résilience des territoires, en lien avec les entreprises de vidéoprotection et le SGDSN, mais ce dernier n'est pas notre interlocuteur principal à l'heure actuelle. Dès lors, il pourrait être intéressant de travailler avec cette structure de manière plus régulière. Nous regrettons à ce titre l'absence d'un interlocuteur unique, tant il est vrai que sur ces sujets, nous devons nous adresser à des ministères ou des secrétariats d'État différents en fonction des sujets. De plus, les actions des uns et des autres ne semblent pas forcément toujours coordonnées ; elles peuvent même sembler parfois concurrentes. Je pense notamment à la confusion engendrée par l'existence simultanée des conseillers numériques France Services et des conseillers France Services. Il m'a ainsi fallu du temps pour comprendre qu'il s'agissait d'acteurs différents. En résumé, nous sommes preneurs d'un interlocuteur unique. Si nous ne pouvons pas disposer d'un ministre dédié, il pourrait être intéressant de travailler avec le SGDSN.

Ensuite, les intercommunalités se proposent d'être un espace de mutualisation en fonction des besoins des communes qui les composent. Il nous avait été proposé de prendre une compétence cybersécurité, mais nous ne le souhaitons pas. Nous pouvons en revanche mutualiser des formations et des ressources humaines. Les plans communaux et intercommunaux de sauvegarde constituent ou constitueront des outils qui devraient être améliorés.

La culture partagée et les conseillers numériques France Services représentent une préoccupation portée par Intercommunalités de France et les Interconnectés depuis un certain temps. Nous avons appelé à la pérennisation des conseillers numériques France Services, qui constituent la cheville ouvrière de la transition numérique et de la cybersécurité. Dans mon territoire, la collectivité de communes Lacq-Orthez, nous avons la chance de disposer de six médiateurs numériques. Ils sont salariés par nos soins et ont pour objectif d'accompagner tous les publics, qu'il s'agisse de nos agents, mais également de la population, dans tous les domaines et sur tous les enjeux du numérique, dont la cybersécurité.

Forts de cette expérience, nous nous battons afin que ces conseillers soient *a minima* pérennisés. Hier, nous avons discuté avec les membres de la commission des finances de l'Assemblée nationale pour étudier précisément le financement de cette pérennisation, dans un contexte budgétaire difficile. En effet, ils sont

indispensables à cette transition numérique et il importe de ne laisser personne de côté, d'autant plus que les agences de proximité ont été fermées. Selon une étude, l'État enregistrerait une perte de 1,6 milliard d'euros si les personnes n'étaient pas accompagnées d'une manière ou d'une autre.

Quel est le bon échelon ? Intercommunalités de France souhaite travailler sur cette directive NIS 2 et que ses membres y soient intégrés, quitte à établir quelques aménagements. Je partage les propos de Mme Saint-Paul concernant le mode opératoire à partir de portes dérobées. À titre d'exemple, une école de commerce a été attaquée, puis le problème s'est répandu aux autres écoles appartenant au même réseau, s'est diffusé à la chambre de commerce et d'industrie dont dépendait l'école et a finalement impacté fortement un aéroport. Il est possible d'imaginer qu'une petite commune serve de point d'entrée pour diffuser une attaque vers la communauté de communes, l'agglomération, la métropole et éventuellement un hôpital.

Les échelons locaux sont très importants, mais il est surtout essentiel de se concentrer sur la coordination. Par ailleurs, les intercommunalités et les régions partagent la compétence en matière de développement économique. Il est donc important de veiller à maintenir une relation étroite avec cet échelon régional. J'ajoute que l'échelon départemental n'est pas en reste, puisque nous travaillons avec des structures comme les opérateurs publics de services numériques (OPSN).

En résumé, l'enjeu ne porte pas tant sur l'échelon pertinent, mais sur la manière dont nous arrivons à travailler ensemble, de manière coordonnée, les uns avec les autres, en évitant les effets de concurrence.

Mme Constance Nebbula. Monsieur Gassilloud, vous avez évoqué le principe de subsidiarité et la nécessité de laisser la main libre aux collectivités. Je salue cette attention, mais souligne que la cybersécurité demeure malgré tout un sujet régalien. Il ne faudrait pas que l'État profite de la discussion en cours pour se désengager de sa mission. Je considère également qu'il ne revient pas aux collectivités locales de s'occuper de la cybersécurité des autres collectivités. De notre côté, nous avons opéré le choix d'accompagner notre cible préférentielle, c'est-à-dire le monde économique au sens très large. De fait, chaque strate de collectivité dispose de son public et doit intégrer la cybersécurité dans le cadre de ses compétences. En revanche, les domaines régaliens, la coordination, la stratégie, le portage politique et l'interlocuteur unique relèvent bien de l'État. Au-delà, je partage moi aussi l'idée d'un nécessaire développement d'une culture du risque du cyber et du numérique.

Aujourd'hui, les collectivités locales payent les conseillers numériques, faute d'avoir pu trouver des solutions pérennes au niveau national. Ici aussi, nous nous débrouillons, face à l'absence de pérennité du dispositif. Chaque conseiller numérique intègre ainsi la dimension cyber dans son accompagnement.

Vous avez ensuite évoqué les moyens organisationnels. Nos collectivités sont confrontées à un problème de compétence et de recrutement. Les métiers de RSSI sont nouveaux pour les collectivités et les experts cyber ne sont pas incités à travailler dans le public, puisqu'ils peuvent être bien mieux rémunérés dans le privé. En outre, les assurances rechignent à assurer les risques cyber. Pourquoi voudraient-elles assurer un risque qui se matérialisera de toute manière ? Par exemple, la métropole d'Angers n'est plus couverte dans certains domaines. Nous avons réouvert des marchés, mais aucun assureur n'a voulu y répondre. Comment agir dans de tels cas ? Faut-il obliger les assureurs ?

Encore une fois, je considère que l'échelon régional est le plus intéressant pour la cible économique que constituent les TPE, les PME et les petites et moyennes entreprises (PMI). J'aimerais qu'un interlocuteur unique existe, mais pour y parvenir, il faudrait des moyens, une ambition, une coordination nationale. Malheureusement, je pense qu'il est trop tard ; les actions ont été trop éparpillées.

Enfin, il me semble que le SGDSN s'occupe plutôt des infrastructures. Je constate également que nos liens avec ce dernier sont assez lâches. À l'heure actuelle, les relations interministérielles fonctionnent très mal en matière de cyber. Dans ce domaine, il n'existe pas d'interlocuteur unique et nous ne savons pas vers qui nous diriger. De la même manière, nous rêverions d'avoir un interlocuteur politique ou administratif unique, mais ceux-ci n'existent pas.

M. Alexandre Ventadour. Ce sujet est effectivement éminemment politique, particulièrement aujourd'hui alors que les problèmes de souveraineté et de géopolitique s'intensifient. Il ne s'agit pas seulement d'attaques crapuleuses, mais bien souvent de tentatives de déstabilisation. Je partage les propos de Mme Nebbula : en matière cyber, le millefeuille administratif a été reproduit, quand nous aurions dû agir en bloc. Lorsque le 17Cyber a été créé, j'avais espoir qu'il constituerait une réponse lisible et unique, mais nous n'en prenons pas véritablement le chemin.

Ensuite, je remercie Mme Saint-Paul pour ses propos concernant les outre-mer. Au-delà de la problématique de l'éloignement de la métropole, les outre-mer constituent des territoires relativement riches, dans des zones souvent relativement pauvres. Elles constituent donc des cibles de choix pour les pirates cybernétiques, comme en témoignent les attaques subies par la Martinique, la Guadeloupe, la Guyane ou La Réunion.

Nous sommes sous-dotés en ressources humaines spécialisées. Mme Nebbula a évoqué les difficultés en matière de recrutement en métropole ; celles-ci sont décuplées dans les territoires ultramarins. À titre d'exemple, il nous a fallu un an et demi pour recruter le RSSI de la collectivité de Martinique. En outre, nos infrastructures sont vieillissantes, éclatées et nous sommes soumis à une forte dépendance vis-à-vis des prestataires. Malgré nos efforts, il est difficile d'en trouver localement et nous devons faire appel à des prestataires situés à plus de 6 000 kilomètres, ce qui contribue à rallonger les délais d'intervention. Néanmoins,

nous avons essayé de trouver des solutions et de nous organiser, notamment sur la partie atlantique des régions ultrapériphériques des départements et régions d'outre-mer ; mais les moyens demeurent insuffisants.

En conséquence, nous préconisons d'inscrire l'outre-mer en « particularité » dans les projections et les propositions pour résorber l'éloignement non seulement kilométrique, mais aussi en termes d'accès à la performance, à la compétence et au financement nécessaire. Nous prônons donc une compensation pour ces territoires, qui sont plus attaqués que les autres.

De son côté, la collectivité de Martinique s'efforcera de continuer à éduquer et sensibiliser les populations à l'utilisation éthique, sécurisée de l'intelligence artificielle. Mais plus les usages de la chose digitale se développent, plus il est nécessaire d'apporter des solutions de sécurité appropriées.

M. Michel Sauvade. Je remercie les députés pour leurs questions, qui témoignent de l'intérêt pour les collectivités locales.

Monsieur Gassilloud, vous avez à juste titre souligné le nécessaire développement de cette culture du risque. Monsieur Saint-Martin, vous avez quant à vous relevé l'importance du portage politique, mais je dois avouer que nos expériences en la matière n'ont pas été forcément toutes concluantes. Je me souviens par exemple d'un chef de cabinet intervenant par visioconférence pour expliquer aux associations d'élus que les conseillers numériques, qui devaient être initialement embarqués à hauteur de 4 000, le seraient finalement à hauteur de seulement 1 500, suscitant par là-même l'incompréhension dans nos rangs.

De fait, il est aujourd'hui difficile de mener des échanges clairs avec le gouvernement sur ces enjeux. À titre d'exemple, j'étais hier à l'Agence nationale de la cohésion des territoires pour une régie, dans le cadre du déploiement de la fibre. Nous avons adressé un courrier au premier ministre, que son directeur adjoint de cabinet a ensuite envoyé à une ministre, qui l'a transféré à un autre ministre, lequel l'a lui-même réadressé à un troisième. Quelque part, quelque chose ne fonctionne pas.

Vous avez posé la question des dispositifs, notamment de l'éducation de la population. Dans cette perspective, le travail de proximité n'a pas forcément vocation à être encadré, dans la mesure où il intervient déjà grâce à une culture partagée entre les grandes municipalités, les grandes communes, les départements, les associations d'élus, les entreprises.

Madame Darrieussecq, votre analogie entre entreprises et collectivités locales est très pertinente, tant l'effet de taille joue. De même, vous avez raison de mettre en lumière les liens numériques entre les différentes collectivités. Par ailleurs, je serais tenté de dire que dans le cadre de la cybersécurité, il n'y a pas une bonne échelle unique, mais des échelles différentes, selon la façon dont le sujet est abordé. Chacun des échelons suit une logique qui lui est propre et la construction législative est confrontée à cette difficulté de devoir raisonner de manière

multiscalaire sur un sujet donné. De fait, il est extrêmement difficile de mettre en place une adaptabilité.

Dans ce domaine, il me semble pertinent de s'inspirer de l'expérience du New Deal Mobile, qui a embarqué les services de l'État, en coprésidence avec les présidents de département et de région, dans des équipes projets, qui nous ont permis de travailler ensemble. Je salue à ce titre le travail bidirectionnel des préfets et regrette qu'il ne soit pas valorisé à sa juste mesure. Il pourrait être approprié de reconstruire quelque chose qui embarque les uns et les autres, de manière réellement opérationnelle.

Ensuite, nous devons nécessairement aborder le principe de réalité en matière de ressources humaines. Dans le département du Puy-de-Dôme, cinq agents se consacrent exclusivement à l'assistance des 8 000 ordinateurs des collèges du département, mais quatre d'entre eux doivent être aujourd'hui renouvelés. En conséquence, le service se retrouve amputé et nous sommes contraints d'alerter les principaux de collèges. Le principe de réalité concerne également la dimension financière. La mutualisation peut être utile en fonction des situations, mais au-delà, l'essentiel concerne l'efficience des investissements. Vos auditions devraient vous permettre d'identifier les points qui permettront d'initier des dynamiques d'entraînement.

Madame Saint-Paul, vous nous avez interrogés sur le seuil des 30 000 habitants. La logique d'harmonisation s'applique aux communes. Il a également été fait mention dans vos questions de la nécessaire acculturation numérique des acteurs. Nous sommes tous frappés d'illectronisme à un moment ou un autre. Qui, dans cette salle, n'a jamais proféré une bordée d'injures parce qu'il n'arrivait pas à valider tel ou tel questionnaire en ligne ?

Cette acculturation doit être initiée par les élus. Une collectivité a par exemple mis en œuvre des messages pièges, à titre de test. La personne qui se fait hameçonner lors de l'exercice se voit ainsi proposer une petite formation. J'ai moi-même été piégé une fois par un hameçonnage malveillant.

En conclusion, au-delà des enjeux numériques dans leur globalité, la cybersécurité est révélatrice des interrogations et des vulnérabilités de notre société. À ce titre, je vous remercie une fois encore pour votre invitation et vos questions, qui confortent notre engagement dans ce domaine, mais également notre volonté d'échanger régulièrement avec les parlementaires. Comme j'ai déjà pu l'évoquer avec certains d'entre vous, il serait certainement utile d'organiser plus régulièrement de tels échanges. De notre côté, nous sommes demandeurs, en tout état de cause.

M. Éric Bothorel, rapporteur général. Pour rebondir sur les propos de Mme Nebbula, il me semble que le monopole de la violence légitime, qui caractérise les missions régaliennes en matière de sécurité, ne peut pas totalement s'appliquer aux enjeux cyber, puisqu'elle concerne la violence physique. De fait, dans le

domaine cyber, les actions d'assistance et de soutien sont majoritairement assurées par des acteurs du privé. La caractérisation même de l'activité de la cybercriminalité et la réparation des dommages subis ne peuvent donc pas reposer uniquement sur l'État, ni sur les collectivités.

Monsieur Sauvade, je souhaite revenir sur les zones touristiques, qui ne peuvent pas être envisagées sans penser aux zones littorales. Pourquoi n'avez-vous voulu réaliser qu'une expérimentation sur la couverture numérique du territoire, alors qu'un dispositif bien plus efficace aurait pu être envisagé dans le cadre du projet de loi sur la certification ?

Vous avez tous souligné par ailleurs que les dispositions du projet de loi devraient être progressives, supportables financièrement et techniquement. Comment y parvenir ? Quelles sont vos propositions concrètes, afin que la mise en œuvre de NIS 2 soit graduelle et progressive ?

M. Thomas Gassilloud (EPR). Je souhaite vous faire part de trois messages. D'abord, la subsidiarité n'équivaut pas au désengagement de l'État. Nous avons besoin de tout le monde pour faire face globalement à la menace. La responsabilité de l'État consiste aussi à indiquer qu'il ne peut pas tout faire à lui seul ; je partage en cela les propos du rapporteur.

Deuxièmement, nous entrons progressivement dans un nouveau monde de conflictualité. À ce titre, notre objectif ne concerne pas uniquement la confiance dans l'économie numérique pour le développement des affaires, mais aussi l'efficacité de notre résilience globale. Je répète que le changement culturel me semble aussi important que la norme.

Enfin, il existe un besoin de clarification dans l'organisation territoriale, concernant les questions de défense. Il faut à ce titre s'appuyer sur un échelon de cohérence dans les territoires, qui pourrait se situer à l'échelle régionale. Par ailleurs, dans ma région, le préfet délégué à la sécurité et à la défense peut jouer ce rôle.

M. Denis Masséglia (EPR). Je partage nombre des questions qui ont été posées par mes collègues et il ne me semble pas opportun de les reformuler. Je tiens également à souligner le travail du Sénat sur l'article 5 *bis*, qui a été intégré dans un premier temps en commission, et qui permet de fournir des moyens financiers et humains aux collectivités territoriales. Je tiens également à remercier l'ensemble des élus aujourd'hui présents pour échanger avec nous sur cet enjeu essentiel.

Vous avez par ailleurs souligné l'intérêt d'un guichet unique à l'échelle gouvernementale. Certains d'entre nous le demandent depuis 2017 et je regrette que l'Assemblée nationale ne se saisisse pas suffisamment de ces sujets de transformation et de transition numérique. Notre société fait en effet face à deux transformations majeures : la transformation écologique et la transformation numérique. N'oublions pas l'une des deux en chemin.

M. le président Philippe Latombe. Nous n'avons pas parlé d'un « éléphant dans la pièce », qui est également issu de l'avis du Conseil d'État. Il concerne les sanctions, que nous n'avons pas abordées jusqu'à présent. En conséquence, je souhaiterais connaître votre point de vue à ce sujet.

Le Conseil d'État estime qu'il y aurait une forme d'iniquité entre le secteur privé le secteur public si le texte n'intégrait pas de sanctions pour le secteur public. Nous pouvons certes comprendre les contraintes budgétaires existantes, mais l'objet consiste bien ici à rehausser le niveau de cybersécurité. Dans le cadre du règlement général sur la protection des données (RGPD), les collectivités se sont assez rapidement conformées aux obligations et n'ont pas été celles qui ont dû subir le plus de sanctions.

Dans la mesure où certaines collectivités et EPA ne montent délibérément pas en puissance en matière de protection cyber, ne faut-il pas envisager des sanctions – y compris non financières – pour les obliger à se conformer aux règles, au-delà du *name and shame* prévu par l'Anssi ?

Mme Constance Nebbula. Monsieur le rapporteur, vous nous avez interrogés sur nos propositions financièrement et techniquement supportables, ainsi que sur leur délai de mise en œuvre. De notre côté, nous estimons que trois ans suffisent. Les régions demeurent des structures consistantes, dotées de budget et de SI structurés ; nous ne sommes pas les plus à plaindre. Le financement concerne pour nous l'outil des CSIRT ; à titre d'exemple, la région Pays de la Loire a mis en place ses propres dispositifs d'accompagnement cyber à partir de ses propres budgets.

En revanche, le financement doit intervenir à partir du moment où il existe une initiative nationale, qui est la même pour tous les acteurs et qui a vocation à être pérennisée sur tous les territoires. Nous souhaitons donc une clarification des outils, qu'il s'agisse de l'outil CSIRT ou de l'outil campus cyber.

S'agissant de la collaboration avec l'État, nous considérons que la préfecture régionale représente la bonne échelle pour échanger et travailler sur les sujets qui nous concernent, à condition que les interlocuteurs soient réceptifs. En revanche, en région, l'Anssi est très efficace ; tous les retours dont nous disposons sont concordants.

S'agissant des sanctions, je me souviens de la norme RGAA (référentiel général d'amélioration de l'accessibilité) sur l'accessibilité numérique, qui avait été votée il y a dix ans dans le cadre d'une loi sur le handicap. Elle oblige les collectivités territoriales à proposer des sites internet accessibles, afin de répondre à la réglementation sur l'accès à l'autonomie. Aujourd'hui, moins de 5 % des collectivités respectent cette norme sans pour autant subir de sanctions. Les collectivités qui commencent la démarche le font sur le seul fondement de leur volonté. À Angers, nous avons ainsi investi plusieurs centaines de milliers d'euros. Dans le même ordre d'idée, l'open data est censée être une obligation légale, mais

seulement 16 % des collectivités la respectent, sans que les autres ne soient pour autant sanctionnées. Ces exemples attestent de fait de l'absence de suivi politique sur les sujets numériques.

Forte de ce constat, j'aurais tendance à penser que la sanction n'est pas une bonne idée. Inversement, il faut trouver des manières d'inciter les collectivités à agir, à travers une ambition politique nationale sur les sujets numériques. Je précise que ces propos concernent plus les petites collectivités que les régions ou les métropoles.

Mme Marlène Le Dieu De Ville. L'accessibilité numérique est un sujet qui évolue, enfin. La loi de 2005 concerne l'accessibilité de tous les outils, non seulement les sites internet, mais plus largement les outils numériques utilisés par des collectivités. À partir du mois de juin 2025, des contrôles de conformité seront menés sur l'ensemble des collectivités et des entreprises soumises au RGAA et des sanctions financières seront appliquées.

Au-delà, s'agissant du texte de loi, il est très difficile d'envisager des sanctions financières, même à trois ans. Il faut d'abord accompagner la montée en compétences des collectivités sur NIS 2 et poser des jalons adaptés à chaque degré. Les métropoles estiment par exemple que le délai de trois ans sera trop court en raison de la complexité du code des marchés publics, qui ne permet pas de changer de prestataire facilement. De fait, des aménagements seront forcément nécessaires, dans le cadre d'une progressivité souhaitable. D'éventuelles sanctions financières ne peuvent intervenir qu'en cas de mauvaise volonté manifeste de la collectivité.

Ensuite, l'enjeu des ressources humaines est effectivement incontournable, mais il est tout aussi difficile de trouver des solutions. Dans mon intercommunalité, notre RSSI, qui avait débuté en alternance va bientôt partir et il sera difficile de le remplacer. Nous ne pouvons pas payer un RSSI, un expert ou un ingénieur à la hauteur de ce qu'il peut prétendre dans le privé.

La soutenabilité financière ne peut être atteinte qu'à l'aide d'un véritable accompagnement financier, semblable à celui que nous avons connu avec le parcours cyber du plan France Relance. Il sera notamment nécessaire de travailler sur un véritable audit.

M. Alexandre Ventadour. Nous sommes très attachés à l'exemption de sanctions pour les régions et les collectivités territoriales, d'abord parce que nous ne maîtrisons pas toujours directement les SI – qui peuvent être sous-traités – et ensuite parce que nous ne disposons pas des mêmes ressources que les entreprises, quelle que soit leur taille, pour recruter les personnes les plus à même de sécuriser nos infrastructures. Nous conduisons déjà des démarches volontaires de sécurisation, avec nos moyens actuels.

Nous portons en notre sein la responsabilité vis-à-vis de nos populations. *De facto*, nous sommes concernés par tout ce qui pourrait porter préjudice aux citoyens ou aux entreprises. S'il s'agit d'enjoindre une région ou une collectivité à

se mettre en conformité, il suffit que la chambre régionale des comptes intervienne. Nous ne pensons pas qu'une sanction financière sur un chiffre d'affaires, qui n'existe pas dans notre cas, constituerait le bon outil. En revanche, nous sommes en mesure d'accepter la mise en place d'audits et la nécessaire mise en conformité, à la suite des résultats de cet audit, dans un laps de temps donné, qui pourrait être par exemple de trois ans. Non seulement nous l'acceptons, mais nous sommes prêts à l'encourager.

Enfin, je considère que la cybersécurité demeure la prérogative de l'État. Les agressions ont évolué depuis un certain temps. Les maux causés de manière virtuelle par les cyberattaques peuvent également se retranscrire de manière assez physique. Dès lors, la protection de la sécurité demeure l'apanage du régalien. En résumé, nous militons pour une exemption de la sanction, mais nous ne préconisons pas une exemption de la responsabilité des collectivités. Cela doit se traduire par un audit, auquel nous nous conformerons, bien évidemment.

M. Michel Sauvade. Comment pouvons-nous agir, concrètement ? Il s'agit de poursuivre les travaux communs, de nous réunir autour d'une même table, sur le plan national et local. Jusqu'à présent, nous avons été écoutés, mais nous n'avons pas été entendus.

Financièrement, nous payons l'absence d'étude d'impact, non seulement l'étude d'impact à date, mais également sur la trajectoire financière, pour autant que nous puissions l'évaluer en fonction de l'augmentation des menaces et des autres vulnérabilités. Simultanément, nous ne disposons pas non plus d'indicateurs ; nous savons uniquement que les moyens ne seront pas à la hauteur de ce que nous attendons. À ce titre, ce sujet doit s'envisager plus largement dans le cadre de la décentralisation des moyens, au plus près du terrain. Cette piste peut sans doute être explorée, à la lumière des propos échangés aujourd'hui par les uns et les autres.

Sur le plan technique, les enjeux de la formation sont patents. Madame Le Dieu De Ville a également mentionné à juste titre les difficultés concernant les recrutements ou les salaires. Dans ce domaine, une véritable réflexion doit être conduite sur notre capacité à nous « muscler » en matière numérique. Cette réflexion doit être conduite, me semble-t-il, à la fois sur le plan national, mais aussi régional. À une certaine époque, dans le domaine du numérique, la France était particulièrement dynamique, en pointe. Cela n'est plus le cas, désormais.

S'agissant de la progressivité, notre réponse est très claire. De notre côté, nous imaginions une marge de progression dans un délai de trois à cinq ans. Cependant, l'Anssi nous a expliqué que la progressivité ne peut pas être prise en compte dans le cadre de la transcription de directives européennes. Nous sommes donc bloqués sur ce point, ce qui est regrettable, dans le cadre d'une réflexion sur l'évaluation et la sanction.

Le simple fait de se poser la question revient déjà s'interroger sur l'efficience de la mise en œuvre de la loi et révèle l'ambiguïté de sa mise en

application. En effet, le questionnement sur la sanction traduit quelque part un échec collectif à embarquer tous les acteurs sur un sujet qui est pourtant essentiel. De son côté, sur d'autres sujets, la Commission nationale de l'informatique et des libertés (Cnil) a prononcé des sanctions lorsqu'il existait une mauvaise volonté manifeste. Or de tels cas demeurent heureusement assez rares. L'AMF ne peut pas se satisfaire d'un cadre de sanctions qui, de toute façon, ne résoudra pas les problèmes.

M. le président Philippe Latombe. Je vous remercie pour vos réponses, votre liberté de ton et d'expression lors de cette table ronde, laquelle ne constitue que le début de nos travaux. Nos interactions se poursuivront.

4. Table ronde réunissant les autorités de régulation financière, mardi 3 juin 2025 à 16 heures 30

Lors de sa réunion du mardi 3 juin 2025, la commission spéciale a organisé une table ronde réunissant les autorités de régulation financière : M. Sébastien Raspiller, secrétaire général de l'Autorité des marchés financiers (AMF), M. Frédéric Hervo, secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR) et M. Alexandre Garcia, chef de service adjoint du service des affaires internationales de l'ACPR.

M. le président Philippe Latombe. Notre cycle d'auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité s'est jusqu'à présent concentré sur les deux premiers titres du texte. Nous abordons aujourd'hui le titre III, qui transpose dans le droit interne les dispositions de la directive européenne sur la résilience opérationnelle numérique du secteur financier ou Digital Operational Resilience Act, dite Dora. Ce volet relève plus particulièrement de la compétence de notre collègue Mickaël Bouloux, rapporteur thématique ici présent.

Le secteur financier constitue une cible privilégiée pour les cyberattaques. Dans son dernier rapport sur la stabilité financière de décembre 2024, la Banque de France soulignait que le risque de cyberattaques demeurait élevé dans un contexte géopolitique dégradé, se manifestant par diverses menaces hybrides. L'Autorité des marchés financiers (AMF) a d'ailleurs intégré la cybersécurité dans ses contrôles et mené trois campagnes thématiques en 2019, 2020 et 2023.

Nous avons le plaisir d'accueillir l'Autorité des marchés financiers (AMF), représentée par M. Sébastien Raspiller, secrétaire général, et l'Autorité de contrôle prudentiel et de résolution (ACPR), représentée par M. Frédéric Hervo, secrétaire général adjoint et M. Alexandre Garcia, chef de service adjoint du service des affaires internationales.

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi) a exprimé des réserves quant à la simplification opérée par le Sénat concernant l'articulation entre Dora et la directive *Network and Information Security 2* (NIS 2). Il estime que la suppression de la notification des incidents à

l'Anssi au profit d'une notification unique aux autorités de contrôle Dora pourrait entraîner des retards préjudiciables, l'Anssi disposant d'un service opérationnel fonctionnant 24 heures sur 24 et 7 jours sur 7, contrairement à l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Autorité des marchés financiers (AMF). Partagez-vous cette analyse ? Une double notification via un formulaire unique pourrait-elle constituer une solution plus appropriée ?

M. Frédéric Hervo, secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR). La résilience cyber et informatique constitue une priorité absolue pour la stabilité financière en France et en Europe, mobilisant quotidiennement nos équipes.

Le secteur financier est en effet confronté à deux défis majeurs dans ce domaine. Tout d'abord, la digitalisation croissante des services financiers, illustrée par l'avènement des paiements instantanés, de la blockchain et de l'intelligence artificielle, a profondément transformé le paysage financier. Cette évolution s'accompagne d'une externalisation accrue des services supports auprès de prestataires spécialisés, notamment dans le domaine du cloud *computing* et des centres de données. La concentration de ces prestataires, souvent des géants technologiques non européens, soulève des enjeux critiques pour le secteur financier. Le cadre réglementaire Dora est donc essentiel, car il confère aux autorités européennes de supervision, en collaboration avec la Banque centrale européenne et les autorités nationales, des pouvoirs de surveillance sur ces acteurs critiques.

Ensuite, nous observons une recrudescence constante des cyberattaques visant le secteur financier, cible privilégiée des cybercriminels. Un établissement financier insuffisamment protégé peut voir sa solidité financière compromise par une attaque d'envergure. À titre d'exemple, la banque chinoise ICBC a dû recapitaliser sa filiale américaine à hauteur de plusieurs milliards de dollars à la suite d'une attaque par rançongiciel l'année dernière.

Dans ce contexte, le règlement Dora instaure un dispositif reposant sur le triptyque tester, alerter, protéger. Il impose un socle commun d'exigences en matière de gestion des risques informatiques et cyber à l'ensemble des acteurs financiers, des banques aux assureurs, en passant par les infrastructures de marché et les émetteurs de cryptoactifs. Chaque entité doit évaluer sa cyber-résilience, les établissements les plus systémiques étant soumis à des tests d'intrusion renforcés pilotés par leur autorité de contrôle.

Dora prévoit également un cadre harmonisé pour la déclaration et le traitement des incidents cyber. Bien que le règlement soit déjà en application depuis le 17 janvier dernier, sa transposition en droit français nécessite certains ajustements. L'ACPR soutient deux amendements qu'elle juge indispensables pour garantir la cohérence et l'efficacité du dispositif de cyber-résilience.

Le premier concerne l'assujettissement des sociétés de financement. Relevant d'un statut national, elles ne sont en effet pas couvertes par le règlement

européen. Cependant, compte tenu de leur rôle crucial dans le secteur bancaire français, il est impératif de leur appliquer les exigences de Dora dans les meilleurs délais. La version adoptée par le Sénat ne prévoit cette application qu'en 2030, ce qui pourrait créer une vulnérabilité pour l'ensemble du secteur financier. À titre d'exemple, Crédit Logement, acteur majeur du crédit immobilier, cautionnait 420 milliards d'euros d'encours en 2024. Or un vol de données personnelles concernant les crédits immobiliers de millions de Français aurait un impact considérable. Face à ce risque, nous préconisons une mise en application rapide du règlement, au moins pour les sociétés de financement les plus critiques. Pour les entités de moindre envergure, nous suggérons une application en janvier 2027, ce qui nous paraît être un délai raisonnable, intervenant deux ans après l'entrée en vigueur du texte.

Concernant l'interaction entre les autorités de contrôle du secteur financier et l'autorité en charge de la cybersécurité dans la gestion des cyberattaques, nous sommes favorables à la mise en place d'une notification parallèle, comme l'autorise le règlement Dora. Cette option permettrait aux établissements d'adresser simultanément leur déclaration d'incident cyber à l'autorité compétente au titre de la directive NIS. Le coût supplémentaire pour les établissements serait nul, puisqu'ils transmettraient les mêmes informations à l'Anssi et à l'ACPR, selon un format identique. En revanche, le gain en termes de stabilité financière serait significatif, chaque heure étant cruciale dans la neutralisation d'une cyberattaque.

L'idée d'une notification unique serait contre-productive, car elle ralentirait le traitement de la menace cyber. Une double notification est au contraire essentielle, car les autorités du secteur financier et l'Anssi ont des missions distinctes. Les unes traitent les conséquences d'un incident cyber pour le secteur financier, notamment la protection de la clientèle, la sauvegarde des avoirs et la gestion du risque systémique, tandis que l'autre se concentre sur la réponse technique à la cyberattaque. Ce double circuit de notification est donc crucial pour une gestion efficace des incidents.

M. Sébastien Raspiller, **secrétaire général de l'Autorité des marchés financiers (AMF).** Comme l'a souligné Frédéric Hervo, les autorités du secteur financier sont responsables de la mise en œuvre du règlement Dora, dans le respect des compétences respectives de l'ACPR et de l'AMF.

Dora représente un élargissement significatif du périmètre de supervision de l'AMF. Nous sommes en effet désormais chargés de superviser la conformité au règlement des sociétés de gestion, des prestataires de services de financement participatif et des prestataires de services sur actifs numériques. Cette population d'acteurs, nombreuse et majoritairement composée d'entités de petite taille, diffère sensiblement du secteur bancaire et assurantiel. Notre défi majeur consiste à nous assurer de la capacité de ces acteurs à satisfaire les exigences ambitieuses du règlement Dora.

J'ai personnellement participé à la finalisation des négociations du paquet Dora sous la présidence française de l'Union européenne. Le processus législatif au niveau communautaire est pratiquement achevé, avec un seul texte de niveau deux restant à adopter. La mise en œuvre représente maintenant un défi considérable, particulièrement pour les entités de taille modeste.

Notre priorité est d'accompagner ces acteurs, en leur expliquant l'importance cruciale de ces mesures pour réduire la probabilité d'incidents majeurs et en limiter les conséquences. Cela nécessite une montée en compétences significative, non seulement pour l'AMF, mais aussi pour nos homologues européens et les autorités en charge des banques et des assurances. Il s'agit d'un effort collectif, car la résilience globale du système dépend de son maillon le plus faible.

Des exemples récents ont démontré qu'une cyberattaque sur un acteur peut avoir des répercussions en cascade sur de nombreux autres. Il est donc primordial que chaque acteur établisse une cartographie précise de ses vulnérabilités, en tenant compte notamment de l'externalisation croissante des systèmes d'information et d'autres prestations essentielles.

Le règlement Dora introduit également l'obligation de réaliser des tests d'intrusion pour les entités critiques à partir du second semestre. Cela exige de l'AMF l'acquisition de compétences très pointues en matière de cyber-expertise, combinées à une connaissance approfondie des acteurs et des métiers du secteur financier. C'est un véritable défi, car ces compétences sont rares et recherchées, et nous devons rivaliser avec le secteur privé pour attirer ces profils, malgré nos contraintes de service public.

Je tiens à souligner l'aspect très opérationnel de la mise en œuvre de ce règlement qui, s'il est correctement appliqué, devrait significativement renforcer la confiance dans le système financier. Les acteurs conscients des risques pour leur survie, la continuité de leurs activités et leur réputation accueillent favorablement ce cadre visant à améliorer le niveau minimum de résilience parmi les acteurs financiers.

Enfin, je rejoins Frédéric Hervo dans son soutien à la double notification. Bien que le terme « double » puisse suggérer une charge de travail supplémentaire, il s'agit en réalité pour un acteur victime d'une cyberattaque de demander de l'aide simultanément à son superviseur et à l'Anssi. Cette approche ne représente pas une charge significative et garantit une réaction rapide et efficace. Il est crucial que l'Anssi soit informée directement et rapidement, sans intermédiaire qui pourrait ralentir le processus. Nous apporterons notre expertise spécifique en complément, mais sans entraver la communication directe entre l'entité attaquée et l'Anssi.

M. Éric Bothorel, rapporteur général. Depuis le 17 janvier 2025, comme vous l'avez rappelé, les entités financières sont tenues de notifier les incidents majeurs. Cette obligation concerne les établissements de crédit, les établissements

de paiement, les prestataires de services d'information sur les comptes, ainsi que les établissements de monnaie électronique. Ils doivent déclarer les incidents opérationnels ou de sécurité liés aux paiements.

J'aimerais connaître les premiers retours sur cette mise en œuvre. Avez-vous déjà identifié des éléments à modifier ou à améliorer dans le cadre de la loi ?

La Banque de France évalue conjointement avec l'ACPR les vulnérabilités du système financier. Elle œuvre également au renforcement de la résilience et de la sécurité du secteur en veillant à la sécurité et à la robustesse de la place financière. Par ailleurs, la Banque de France contribue à la transformation numérique du secteur en travaillant sur l'euro numérique, la monnaie numérique de banque centrale, et l'infrastructure du marché des capitaux.

Le dernier rapport d'analyse des risques encourus par le système financier souligne que le secteur financier demeure résilient face au risque cyber grâce à ses investissements continus en cybersécurité et sa préparation aux attaques. Néanmoins, de mauvaises pratiques de cybersécurité entraîneraient 2,6 fois plus d'incidents cyber répertoriés et des pertes financières conséquentes, sans compter le risque de réputation et les fuites d'information. Êtes-vous convaincus de l'adéquation du niveau de préparation et de protection actuel ?

Enfin, partagez-vous la position de l'Association de management des risques et des assurances de l'entreprise (Amrae) selon laquelle, pour bénéficier de la couverture d'assurance, il conviendrait de notifier l'incident non pas au moment de sa détection, mais lors de sa présentation à l'assurance ?

M. Mickaël Bouloux, rapporteur. J'ai l'honneur d'être le rapporteur thématique pour le titre III du projet de loi qui porte sur la résilience opérationnelle numérique du secteur financier et transpose la directive Dora du 14 décembre 2022. J'ai noté ce matin, lors de la réunion qui s'est tenue avec la direction générale du Trésor que nous retrouvons des thématiques communes, notamment concernant le formulaire de notification aux entités. J'aurai également l'occasion de rencontrer la Fédération bancaire française en fin de semaine. J'ai bien pris note de vos recommandations concernant les sociétés de financement de type Crédit Logement. Nous avons également discuté avec le Trésor de la question du signalement des incidents. Vous avez déjà abordé la question du double assujettissement entre Dora et NIS 2, du moins pour cette partie relative aux notifications. Si vous identifiez d'autres points de chevauchement, je suis intéressé de les connaître.

Quels obstacles avez-vous pu identifier dans la mise en application du règlement Dora ? Je fais référence à la fois à sa mise en œuvre par les entités financières que vous supervisez, mais aussi par votre propre institution, étant donné que le règlement comporte un certain nombre d'obligations et de changements qui vous concernent également. J'ai bien noté que vous avez évoqué notamment le sujet des ressources humaines et l'accès aux compétences en cybersécurité, un enjeu qui sera largement partagé.

Concernant l'articulation entre la directive et le règlement, pensez-vous que ces deux textes européens sont suffisants pour protéger notre système financier contre les risques liés aux technologies de l'information et de la communication ? Envisagez-vous des étapes supplémentaires ou des améliorations ?

Enfin, quel rôle avez-vous joué lors de l'élaboration de ces textes ? Avez-vous le sentiment d'avoir été écoutés lors des négociations en amont de cette législation européenne ?

Mme Anne Le Hénanff, rapporteure. Pourriez-vous dissiper les inquiétudes exprimées par certains acteurs auditionnés concernant le risque de double assujettissement à NIS 2 et Dora, en particulier au regard de l'article 43A introduit par le sénateur Canevet au Sénat ?

Par ailleurs, il me semble que certains groupes bancaires intègrent désormais la notion de cybersécurité pour leurs propres clients. Votre intervention s'étend-elle jusqu'à ce niveau ? Accompagnez-vous les organismes bancaires dans leur relation avec leurs clients en matière de cybersécurité ? Si c'est le cas, de quelle manière procédez-vous ?

Étant donné que certaines banques ont déjà établi des critères d'exigence en matière de cybersécurité pour leurs clients, ne pensez-vous pas que Dora pourrait agir comme un stimulateur, un moteur, voire une opportunité, ou avoir un effet d'entraînement vis-à-vis du client final ? Je serais très intéressé de connaître votre analyse de l'impact de Dora jusqu'au bout de la chaîne.

Mme Catherine Hervieu, rapporteure. Vous avez évoqué la question des cryptomonnaies et des monnaies numériques. Je souhaiterais apporter quelques précisions en lien avec les développements au sein de l'Eurosystème et le projet d'émission d'une monnaie virtuelle complémentaire aux espèces et aux autres moyens de paiement. Dans cette perspective, l'euro numérique pourrait être déployé à partir de 2027 ou 2028.

Concernant les cryptomonnaies, certains acteurs économiques souhaitent développer leur utilisation, ce qui soulève des questions malgré la mise en application du règlement sur les marchés de crypto-actifs (Mica) par l'Union européenne, visant à assurer la stabilité des entreprises crypto et la protection des consommateurs.

Vous avez souligné dans vos propos introductifs la rapidité exponentielle de la digitalisation, qui nous pose des défis constants. À cet égard, il est important de noter qu'en 2021, 70 % des cyberattaques et des rançongiciels officiellement recensés exigeaient un paiement en cryptomonnaies, dont le célèbre bitcoin pour 60 % d'entre eux.

Dans ce contexte, le travail sur la transposition de la directive européenne pour sécuriser à la fois les infrastructures sensibles et critiques, les aspects financiers et les aspects cyber revêt une importance capitale. En tant que rapporteure pour le

titre Ier, je suis particulièrement sensible à ces enjeux, d'autant plus que la problématique de fond reste la fragilisation potentielle des États.

Selon vous, quels moyens peuvent être mis en œuvre pour tracer efficacement les attaques, sécuriser l'ensemble du système et mettre en place des mesures de lutte anticipant ces évolutions technologiques qui s'accélèrent de manière exponentielle ?

M. Frédéric Hervo. D'après nos premières expériences en matière d'incidents et de leur notification, il convient de souligner l'apport majeur de Dora. Ce règlement établit un cadre harmonisé pour le reporting et la notification des incidents, ainsi que pour leur traitement coordonné entre autorités, tant au niveau national qu'européen. Dora prévoit notamment un mécanisme de gestion des incidents majeurs susceptibles d'avoir un impact à l'échelle européenne.

Selon les dispositions de Dora, les incidents majeurs, définis selon des critères spécifiques énoncés dans le règlement, doivent être notifiés aux autorités compétentes dans un délai de quatre heures après leur qualification comme majeurs, et au plus tard vingt-quatre heures après leur survenance. Ce dispositif est entré en vigueur le 17 janvier dernier.

Au 2 juin 2025, l'ACPR a reçu 76 notifications d'incidents majeurs. Ce chiffre, bien que significatif, doit être nuancé pour deux raisons principales. Tout d'abord, un même incident a pu faire l'objet de notifications multiples par plusieurs entités affectées. L'incident Harvest, largement médiatisé et ayant impacté plusieurs entités financières, en est un exemple probant. Ensuite, nous sommes au début de la mise en œuvre de ce dispositif. Certains acteurs ont donc tendance à notifier par précaution, même lorsqu'ils ne sont pas entièrement certains du caractère majeur de l'incident.

Concernant la typologie des incidents signalés, près de la moitié sont liés à des défaillances informatiques opérationnelles, ce qui relève des problématiques classiques de continuité opérationnelle. Un quart concerne des incidents de paiement et un autre quart est d'origine cyber, incluant notamment l'incident Harvest, qui a mis en lumière l'importance cruciale de la chaîne d'externalisation dans la vulnérabilité potentielle des systèmes.

Les premiers retours d'expérience démontrent l'utilité indéniable de ce dispositif de notification, bien que nous soyons encore dans une phase d'apprentissage. Il permet aux autorités d'avoir rapidement une visibilité sur les entités du secteur financier affectées, facilitant ainsi la coordination de la réponse entre les différentes autorités, y compris l'Anssi, et la communication avec les entités impactées.

Ce dispositif ne remplace pas les mécanismes préexistants. Dora vient normaliser et harmoniser ces pratiques, en établissant des attentes claires en termes de délais et de procédures.

Jusqu'à présent, nous n'avons pas eu à traiter d'incident majeur à l'échelle européenne. La plupart de ceux qui ont été signalés ont une portée nationale et sont généralement résolus rapidement, en particulier quand ils sont liés à la continuité opérationnelle. Bien que nous soyons toujours en phase d'apprentissage, Dora démontre déjà toute son utilité dans la gestion et la coordination des incidents au sein du secteur financier.

M. Sébastien Raspiller. Pour compléter ces informations du point de vue de l'AMF, nous avons reçu une trentaine de notifications depuis la mise en œuvre de Dora mi-janvier. La répartition est la suivante : 40 % concernent des cyberattaques, environ la moitié sont liées à des problèmes de disponibilité des services informatiques et 10 % relèvent de pannes basiques.

Le nombre de notifications est relativement significatif, d'autant plus que nous avons observé un temps d'adaptation nécessaire pour les acteurs, particulièrement ceux de plus petite taille, afin qu'ils comprennent et appliquent correctement les nouvelles exigences de notification standardisée. Nous constatons une amélioration progressive : les notifications arrivent désormais dans les délais impartis et respectent le format requis. Bien que l'apprentissage soit toujours en cours, nous notons une amélioration sensible. Les acteurs semblent également avoir intégré qu'il est préférable de notifier de manière prudente plutôt que d'attendre d'être absolument certains de la nécessité de le faire.

M. Frédéric Hervo. Concernant l'état de préparation de la place financière, et selon la perception que nous pouvons avoir de l'ensemble de la chaîne, il est important de souligner la maturité relative du secteur financier en matière de cybersécurité. Elle s'explique notamment par le fait que ce secteur figure parmi les plus ciblés par les cyberattaques, ce qui a conduit à une sensibilisation accrue depuis longtemps.

Dora apporte une approche homogène pour l'ensemble du secteur financier, unifiant des réglementations qui étaient auparavant sectorielles. Cependant, nous ne partons pas de zéro. Le premier pilier de Dora, qui concerne l'analyse des risques propres à chaque institution, l'identification de ses vulnérabilités, la mise en place de différents niveaux de contrôle et l'implication de la gouvernance, s'appuie sur des concepts déjà bien établis.

L'aspect le plus novateur de Dora, qui nécessitera un travail important de la part des acteurs cette année, concerne l'introduction de clauses-types obligatoires dans les contrats d'externalisation avec les prestataires critiques. Cet élément est crucial, notamment dans le contexte de l'utilisation croissante des services de *cloud computing*, où le pouvoir de négociation des établissements financiers face aux géants technologiques était souvent limité. Ces clauses standardisées renforcent la position des acteurs du secteur financier vis-à-vis de ces prestataires, souvent extérieurs à l'Union européenne.

Notre rôle en tant qu'autorités a été essentiel dans la sensibilisation à ces nouvelles dispositions. Nous avons organisé de nombreuses réunions avec les associations professionnelles pour expliquer les implications de Dora, notamment en ce qui concerne les tests d'intrusion. Dora exige en effet que les entités mettent en place leur propre plan de tests d'intrusion à terme, ce qui représente un changement significatif dans leurs pratiques de cybersécurité.

Le principe de proportionnalité s'applique à l'ensemble des acteurs soumis à Dora. Pour un sous-ensemble plus restreint d'entités critiques ou systémiques, des tests sous le contrôle des autorités de supervision seront mis en place. Ces tests visent à détecter les points de vulnérabilité dans les systèmes critiques pour les services financiers, à l'instar d'un hacker externe.

Nous commencerons à déployer ce dispositif très exigeant en termes d'expertise et de ressources à partir du second semestre, sur un cycle triennal. Il est évident que les plus petits acteurs ou certains secteurs, notamment l'assurance et les mutuelles, plus dispersés, partent de plus loin en termes de sensibilisation. Notre approche sera progressive, pragmatique et proportionnée, privilégiant l'accompagnement avant le contrôle.

Concernant les clients, nous constatons des liens importants avec la fraude, particulièrement celle liée aux paiements. Il est crucial de rappeler les bonnes pratiques de prévention à la clientèle, d'autant plus que l'évolution technologique, notamment l'utilisation de l'intelligence artificielle, facilite certains dispositifs frauduleux.

Dora souligne à juste titre l'importance d'une prise en compte rigoureuse de toute la chaîne des prestataires externes dans le cadre de l'externalisation. L'incident Harvest illustre parfaitement cette nécessité : la cyberattaque qui a affecté ce fournisseur de logiciels pour de nombreux acteurs, dont des conseillers en gestion de patrimoine, provenait en réalité d'un de ses propres prestataires. Cet exemple démontre l'importance de considérer l'intégralité de la chaîne de sous-traitance et d'externalisation.

Dora représente indéniablement une avancée significative. Cependant, les menaces continuent d'évoluer, et il est impératif de réduire l'avance des organisations criminelles ou para-étatiques. Une évaluation de Dora sera nécessaire après quelques années d'application.

Concernant l'articulation entre NIS 2 et Dora, deux points méritent d'être soulignés. Tout d'abord, Dora étant un texte spécialisé, une entité du secteur financier répondant à ses exigences n'est pas soumise à NIS 2, ce qui constitue une simplification. Ensuite, la double notification des incidents est une nécessité opérationnelle. Bien que nous partagions les notifications reçues avec diverses autorités, y compris au niveau européen, il est crucial que l'Anssi, en tant qu'autorité responsable, reçoive directement ces notifications, même si cela implique un doublon. Cette approche nous permet de gagner un temps précieux dans la réponse

aux incidents, sans remettre en cause le principe général selon lequel NIS 2 ne s'applique pas au secteur financier, Dora étant la loi spéciale en la matière.

M. Sébastien Raspiller. L'AMF est chargée de l'agrément des prestataires de services sur actifs numériques et assumera également la supervision de ces acteurs dans le cadre de Dora. Ces entités, déjà familiarisées avec certaines exigences grâce au régime national issu de la loi Pacte, sont souvent des acteurs conséquents et intrinsèquement digitaux, opérant à l'échelle européenne et internationale.

Nous avons récemment observé des incidents majeurs de vol de données et de cryptoactifs, comme celui survenu en février sur une plateforme internationale, impliquant 1,6 milliard de dollars. Il est à noter que cette plateforme n'était pas autorisée à opérer en France, n'étant pas enregistrée conformément à la loi Pacte. Notre vigilance a permis d'éviter que des clients français ne soient affectés par ce piratage.

Bien que le règlement Mica n'ait pas retenu l'obligation d'un audit cyber réalisé par un prestataire certifié, contrairement à ce que prévoyait la loi Pacte, nous encourageons vivement les acteurs à maintenir cette pratique. De nombreux opérateurs le font spontanément, conscients de l'importance de cette démarche pour la confiance de leurs clients.

Les prestataires de services sur actifs numériques sont pleinement intégrés dans le champ d'application de Dora, avec une exposition particulièrement élevée aux risques de cyberattaques. Nous observons généralement une bonne maturité chez ces acteurs en France, mais ce niveau peut varier à travers l'Union européenne et au-delà. Le passeport européen prévu par le règlement Mica rend d'autant plus crucial le renforcement des exigences en matière de cybersécurité au niveau européen.

Concernant l'articulation entre NIS 2 et Dora, nous saluons la mise en place d'un point d'entrée unique pour les autorités de supervision financière, ce qui simplifie les procédures et évite les doublons. Cette approche est particulièrement pertinente pour les acteurs sous supervision conjointe, comme certaines infrastructures de marché supervisées à la fois par la Banque de France et l'AMF.

Quant à l'efficacité de Dora, il est prématuré d'envisager une version ultérieure. L'objectif n'est pas d'atteindre un monde sans cyberattaques, ce qui est irréaliste, mais de réduire significativement leur occurrence et leurs impacts. Le succès de Dora se mesurera à sa capacité à améliorer les investissements en cybersécurité et à atténuer les effets des attaques lorsqu'elles surviennent.

La résilience est un enjeu crucial pour toute entité consciente des risques cybernétiques. Il s'agit non seulement de savoir y faire face lorsqu'ils surviennent, mais aussi de s'efforcer d'en réduire la fréquence. C'est à l'aune de ces critères que nous pourrons juger de l'efficacité de Dora, bien qu'il soit encore trop tôt pour tirer des conclusions définitives.

Concernant les obstacles, j'ai évoqué précédemment les défis liés aux ressources humaines. Au-delà du recrutement de cyber-experts, nous devons impérativement élever le niveau de compétence de l'ensemble des acteurs impliqués dans la supervision classique. Cette exigence s'applique tant à notre personnel qu'aux gestionnaires externes. Le risque cyber n'étant pas nécessairement leur préoccupation première, il est essentiel qu'ils intègrent pleinement les enjeux de Dora dans leurs pratiques. Cela implique un effort considérable en matière de formation.

À titre d'exemple, nous avons récemment organisé une journée dédiée aux enjeux de Dora pour les équipes de conformité et de contrôle interne, rassemblant 450 participants. Nous proposons également des webinaires d'accompagnement. Notre objectif est de rendre ces informations accessibles non seulement aux cyber-experts, mais aussi à un public plus large dont ce n'est pas le cœur de métier. C'est un véritable défi que nous devons relever.

Un autre enjeu majeur concerne la mise en place des couches nationales prévues par Dora. Bien que nous bénéficiions d'une excellente coordination avec l'autorité nationale, la dimension européenne ajoute un niveau de complexité. Les trois autorités européennes de supervision devront se coordonner efficacement, ce qui représente une nouveauté potentiellement source de difficultés. Il sera crucial de s'assurer du bon fonctionnement de cette collaboration.

Quant à savoir si l'Autorité a été écoutée lors de l'élaboration de Dora, je peux témoigner, pour avoir été de l'autre côté, que j'ai consacré un temps considérable à l'écoute des dix autorités concernées. J'ose espérer qu'elles ont été non seulement entendues, mais aussi écoutées. Cependant, il leur appartiendra d'en juger.

Le débat le plus ardu a porté sur les fournisseurs de cloud et la possibilité d'une extra-territorialité. Mais la question ne se limite pas à ce seul aspect. D'autres fournisseurs de données, par exemple, peuvent également avoir un impact systémique considérable. Prenons le cas de la gestion d'actifs basée sur des indices : une erreur dans le calcul de ces indices pourrait avoir des conséquences désastreuses pour les clients et les épargnants.

J'ai observé une évolution dans l'attitude des prestataires tiers critiques. Alors qu'ils exerçaient un lobbying intense lors des négociations politiques initiales, ils semblent aujourd'hui avoir accepté l'inévitabilité de leur inclusion dans le périmètre de Dora. Ils demandent désormais des clarifications pour se mettre en conformité, ce qui témoigne d'une compréhension accrue des bénéfices potentiels de cette réglementation, notamment en termes de justification des investissements nécessaires en interne.

En conclusion, au-delà des obstacles identifiés, ces évolutions constituent des facteurs de réussite potentiels pour la mise en œuvre efficace de Dora.

M. le président Philippe Latombe. Des questions se posent quant à l'articulation le règlement général de protection des données personnelles (RGPD), la Commission nationale informatique et libertés (CNIL) et Dora. Si l'architecture entre NIS 2 et la CNIL est clairement définie, qu'en est-il de la relation entre Dora et la CNIL ? En tant qu'autorité de référence pour le secteur financier, comment gérez-vous les incidents cybernétiques ayant un impact sur les données personnelles ? Existe-t-il une coordination particulière avec la CNIL dans ces situations ?

Mme Laetitia Saint-Paul (HOR). Vous avez indiqué que l'intelligence artificielle (IA) facilitait les dispositifs de fraude. Pourriez-vous nous éclairer sur la manière dont les cybercriminels exploitent concrètement l'IA ? Par ailleurs, comment l'utilisez-vous de votre côté à des fins défensives, sachant que les criminels ont souvent une longueur d'avance ?

Pouvez-vous préciser dans quelle mesure les cryptomonnaies facilitent ou non le blanchiment d'argent ? Face à l'adage « suivez l'argent » souvent cité en matière de criminalité, quels sont les nouveaux moyens développés pour contrer ce blanchiment, notamment dans le contexte des cryptomonnaies ?

Enfin, vous avez indiqué que 70 % des cyberattaques étaient des attaques par rançongiciel. Pourriez-vous détailler la répartition des 30 % restants ?

M. Sébastien Raspiller. Concernant l'articulation entre Dora et le RGPD, notre rôle de superviseur nous amène à vérifier que les entités assujetties respectent l'ensemble des réglementations applicables. Ainsi, lorsqu'une fuite de données personnelles est signalée dans le cadre de Dora, nous nous assurons que l'entité a bien effectué les déclarations nécessaires auprès de la CNIL, conformément au RGPD. Cette procédure est désormais bien intégrée dans les pratiques des entités supervisées. À ce jour, nous n'avons pas identifié de difficultés majeures dans cette articulation entre Dora et le RGPD. Si des problèmes devaient survenir, ils seraient traités dans le cadre de notre dialogue de supervision.

Concernant l'utilisation de l'IA dans les fraudes, nous observons effectivement une recrudescence inquiétante. Selon les études de l'AMF, 15 % des Français estiment avoir été victimes ou cibles d'une tentative d'arnaque financière, ce chiffre atteignant 35 % chez les moins de 35 ans. Bien que le nombre d'arnaques effectives soit inférieur, la tendance est préoccupante avec une multiplication par trois sur les trois dernières années.

Parmi ces fraudes, certaines exploitent déjà l'intelligence artificielle, notamment à travers l'utilisation de *deepfakes*. Ces techniques permettent de manipuler l'image et la voix de personnalités connues pour leur faire tenir des propos qu'elles n'ont jamais prononcés, créant ainsi des publicités trompeuses mettant en scène des journalistes, des hommes politiques ou des célébrités du sport.

Face à cette menace croissante, notre action se déploie sur plusieurs fronts. Nous multiplions les alertes pour sensibiliser le public et nous transmettons

systématiquement les cas détectés aux autorités judiciaires compétentes. Néanmoins, nous sommes conscients que le développement de l'IA continuera d'amplifier ce phénomène, nécessitant une vigilance accrue et des moyens de lutte toujours plus sophistiqués.

Bien que l'imitation ne soit pas encore parfaite, les progrès rapides accomplis pour générer des avatars laissent présager une amélioration significative de la qualité dans un avenir proche. Nous travaillons activement sur l'utilisation de l'IA pour nous protéger contre ces technologies de manipulation. Il est vrai que le secteur privé a souvent une longueur d'avance, mais je ne peux pas totalement abonder dans votre sens en tant que superviseur.

Il est indéniable que la lutte contre ces technologies représente un défi majeur. Les autorités doivent impérativement investir dans des moyens de détection adéquats pour ne pas se laisser distancer. Parallèlement, des mesures plus basiques s'avèrent essentielles. Nous avons ainsi lancé une campagne d'éducation financière axée sur un principe fondamental : il n'est jamais urgent de perdre de l'argent. L'objectif est d'inciter à la prudence face aux offres alléchantes assorties de délais artificiellement courts. Ces réflexes élémentaires doivent être constamment rappelés.

La technologie jouera un rôle crucial dans la lutte contre des manipulations de plus en plus sophistiquées, mais elle doit s'accompagner d'approches préventives et éducatives. Concernant les cryptoactifs, l'AMF a hérité de compétences élargies, notamment en matière de lutte contre le blanchiment, conformément à la loi Pacte. Si la traçabilité inhérente à la blockchain est un atout, l'enjeu principal réside dans l'identification des utilisateurs. Le règlement européen révisé sur les transferts de fonds (TFR), entré en vigueur récemment, impose désormais l'identification réelle des parties lors des transferts de cryptoactifs, à l'instar des règles appliquées aux transferts de fonds traditionnels. Cette réglementation vise à garantir une transparence comparable entre les transactions en cryptoactifs et celles en monnaie fiduciaire.

Je souscris pleinement aux propos de Sébastien Raspiller concernant les cryptoactifs et leur vulnérabilité face aux risques de blanchiment. Le règlement Mica, en instaurant un cadre réglementaire pour certaines activités liées aux cryptoactifs, y compris sous l'angle de la lutte contre le blanchiment et le financement du terrorisme, permet de mettre en place un dispositif de contrôle efficace. Bien que ce règlement ne couvre pas l'intégralité du secteur, notamment la finance décentralisée, il constitue une avancée significative.

Concernant l'intelligence artificielle, je souhaite évoquer un autre exemple d'utilisation frauduleuse : la modernisation de la fraude au président. Cette escroquerie classique, où un imposteur se fait passer pour un dirigeant d'entreprise afin d'obtenir un virement urgent, se voit aujourd'hui amplifiée par l'IA. Les fraudeurs exploitent désormais les réseaux sociaux et les techniques d'imitation vocale pour rendre leurs tentatives plus crédibles.

L'IA, comme toute évolution technologique, offre de nouvelles opportunités aux fraudeurs, mais également de nouvelles perspectives pour la lutte anti-fraude. À titre d'exemple, de nombreux établissements financiers commencent à utiliser massivement l'IA pour analyser les flux d'opérations dans le cadre de la lutte contre le blanchiment et le financement du terrorisme (LCB-FT). Ces outils permettent un criblage plus efficace des opérations sensibles et facilitent la préparation des déclarations de soupçon. Certains grands groupes financiers ont déjà mis en œuvre ces technologies, tandis que d'autres en sont encore au stade de l'expérimentation. L'ACPR, qui joue un rôle prépondérant dans la prévention du blanchiment et du financement du terrorisme, évalue actuellement ces évolutions intéressantes sur le principe.

5. Table ronde réunissant des entreprises de cyberdéfense, mercredi 4 juin 2025 à 15 heures 30

Lors de sa première réunion du mercredi 4 juin 2025, la commission spéciale a organisé une table ronde réunissant des entreprises de cyberdéfense : M. Michaël Barthellemy, responsable de la gestion des risques cyber et des actifs d'Airbus et représentant de la commission Cyber du Groupement des industries françaises aéronautiques et spatiales (Gifas), M. Thierry Racaud, président-directeur général d'Airbus Protect, M. Yves Berthe, coordinateur sécurité d'Airbus France, M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing d'Orange Cyberdéfense, M. Vivien Mura, directeur des technologies d'Orange Cyberdéfense, Mme Katuiscia Benloukil, vice-présidente communication de Tehtris et M. Arnaud Dechoux, directeur des affaires publiques de Sekoia.io.

M. le président Philippe Latombe. Mes chers collègues, nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques au renforcement de la cybersécurité se poursuivent aujourd'hui avec une table ronde réunissant des représentants d'entreprises présentes dans les domaines de la cyberdéfense et de la cybersécurité. Cette audition sera donc à la fois consacrée à l'impact de la directive NIS 2 sur les entreprises soumises à la réglementation et sur les services de cybersécurité qu'offrent vos groupes respectifs, notamment aux infrastructures critiques.

Airbus sera représenté par M. Barthellemy, responsable de la gestion des risques cyber et des actifs et représentant de la commission cyber du groupement des industries françaises aéronautiques et spatiales (Gifas), M. Thierry Racaud, président directeur général d'Airbus Protect et M. Yves Berthe, coordinateur sécurité d'Airbus France. M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing, et M. Vivien Murat, directeur des technologies, représentent Orange Cyberdéfense. L'entreprise Tehtris est représentée par Mme Katuiscia Benloukil, vice-présidente communication et Sekoia.io par M. Arnaud Dechoux, directeur des affaires publiques.

Avant de vous céder la parole, je souhaite vous poser une question liminaire. Vos activités sont souvent implantées dans plusieurs pays de l'Union européenne. Comment envisagez-vous de vous adapter aux différents modèles de transposition retenus par les États membres ?

M. Michaël Barthellemy, responsable de la gestion des risques cyber et des actifs d'Airbus et représentant de la commission cyber du Gifas. Je vous remercie de nous accueillir aujourd'hui pour cette audition. La résilience digitale présente plusieurs enjeux cruciaux pour nos organisations, notamment critiques – catégorisées entreprises essentielles ou entreprises importantes –, notre capacité à anticiper, prévenir, dissuader, détecter, retarder, défendre, répondre et résister aux attaques et à nous remettre des incidents de cybersécurité.

Il faut également citer la protection de l'intégrité informatique et fonctionnelle face aux risques croissants ; la limitation des pertes financières, d'image et de confiance en cas d'incident majeur ; la continuité des activités et le maintien de la productivité malgré les attaques et la préservation et la sécurisation des données, y compris dans le cadre du règlement général sur la protection des données (RGPD) et de la loi « informatique et libertés » en France.

Cette résilience, quand elle parvient à être démontrée, conditionne l'instauration d'un climat de confiance avec nos usagers, clients, fournisseurs et autorités de tutelle. Une fois rappelés ces enjeux importants que représentent la résilience digitale et la cybersécurité pour notre filière, je souhaiterais attirer votre attention sur quelques points qui ressortent de notre étude du projet de loi. Sans vouloir déposséder le Parlement français de ses prérogatives, il n'est plus envisageable aujourd'hui que ce type de texte soit du niveau d'une directive européenne. En réalité, il devrait être porté par un règlement européen. Imaginez la difficulté pour un groupe comme Airbus, présent dans la quasi-totalité des États membres de l'Union européenne (UE). Nous allons devoir appliquer vingt-sept réglementations différentes, ce qui engendrera des coûts supplémentaires et posera des complexités techniques.

Ensuite, il faut analyser plus globalement l'impact de la réglementation sur la continuité des dispositifs existants, qui représente pour notre filière une double surtransposition de la directive européenne, comme nous aurons peut-être l'occasion de le démontrer. La France va en effet au-delà des demandes de la directive et la proposition de transposition actuelle vient en doublon d'un certain nombre de contraintes qui sont déjà requises dans le corpus juridique existant : la loi de programmation militaire (LPM), l'instruction générale interministérielle (IGI) n° 1300, l'IGI n° 900 et l'IGI n° 901.

L'augmentation des sanctions fera également peser une pression financière sur nos entreprises, transformant le dispositif existant, qui est fondé sur la coopération et la confiance entre acteurs, en une relation qui sera plus contractuelle. Nos concurrents internationaux, y compris européens, non soumis à ces mêmes règles, seront avantagés, laissant nos entreprises dans une position désavantageuse.

Il faut donc veiller à ne pas créer, par cette surtransposition, une opportunité de « *dumping* de cybersécurité » pour les autres États membres.

En revanche, le véritable risque concerne particulièrement les petites et moyennes entreprises (PME) et les entreprises de taille intermédiaire (ETI), qui sont déjà vulnérables et qui pourraient être fragilisées par des exigences qui seraient trop contraignantes et une mise en œuvre précipitée. En effet, une demande de mise en œuvre trop rapide risquerait de créer chez eux des déséquilibres importants. Leur soutien et leur préservation constituent donc une priorité à laquelle nous devons répondre de manière concrète.

Ensuite, la question de la souveraineté numérique et de l'indépendance géostratégique figure au cœur de nos préoccupations. Parfois, la résilience opérationnelle contredit en partie le principe de souveraineté, notamment sur les aspects liés aux Gafam, qui occupent une place prépondérante. En conséquence, les choix qui sont réalisés aujourd'hui détermineront notre capacité à maintenir l'équilibre entre notre indépendance et nos interdépendances, dans un contexte de concurrence globale.

Enfin, pour que nos entreprises puissent réussir cette transition vers la directive NIS 2 et la résilience, un soutien au bon niveau des services de l'État est indispensable, sous forme technique, financière et d'aide au développement de solutions de confiance adaptées aux PME et aux ETI. Cet investissement permettra d'assurer la pérennité et la compétitivité de notre filière. Nous pensons que l'Agence nationale de la sécurité des systèmes d'information (Anssi) doit jouer un rôle central dans ce dispositif.

Je cède la parole à mon collègue Thierry Racaud d'Airbus Protect, société qui est déjà conduite à supporter notre écosystème et la nation de façon plus générale, sur les sujets de cybersécurité et de cyberrésilience.

M. Thierry Racaud, président-directeur général d'Airbus Protect. Airbus Protect est une société française filiale du groupe Airbus, créée en juillet 2022. La société résulte du regroupement d'activités cyber au centre du groupe et bénéficie ainsi d'un héritage d'excellence et d'une compréhension approfondie des enjeux de la cybersécurité dans les secteurs les plus critiques. La mission d'Airbus Protect consiste à contribuer à la cyberprotection d'Airbus, c'est-à-dire ses produits, ses usines et ses filiales, sa chaîne logistique, sa chaîne de valeur et plus largement le secteur aérospatial, les infrastructures critiques et les institutions nationales et européennes.

Ainsi, à travers Airbus Protect, Airbus met ses meilleurs experts au service de ses sous-traitants, partenaires, clients, partout en Europe. Nos services couvrent l'ensemble du cycle de vie de la cybersécurité en offrant une approche holistique et sur mesure pour répondre aux besoins particuliers de nos clients et partenaires, du conseil à l'audit de cybersécurité, pour les aider à se mettre en conformité avec les règlements nationaux et européens : protection des systèmes critiques, service de

détection et de réponse aux incidents de cybersécurité, cybersécurité des produits, formation et sensibilisation, tests d'intrusion et recherche de vulnérabilité cyber. Les services d'Airbus Protect sont, dans leur majorité, labellisés par l'Anssi. Ainsi, en combinant son héritage industriel avec une expertise pointue en cybersécurité, Airbus est le partenaire cyber du secteur aérospatial. Les salariés d'Airbus Protect, au nombre de 500 en cybersécurité, sont fiers de contribuer à la protection des intérêts stratégiques français.

M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing d'Orange Cyberdéfense. Orange Cyberdéfense, compagnie majoritairement acquise par Orange, est une société de services sur l'ensemble du cycle de la cybersécurité : analyse de la menace propre, détection, protection, remédiation, gestion de crise et conseil. Orange Cyberdéfense traite l'ensemble des segments du marché, les multinationales, les PME et TPE, y compris les clients Orange, c'est-à-dire le *BtoC*.

La société évolue dans un marché extrêmement concurrentiel : nous sommes leaders en France avec 12 % de parts de marché et en Belgique avec 5 %. Dans ce marché très concurrentiel, nos clients font face à trois complexités. La première a trait à une menace toujours évolutive en degré. L'Europe continue à souffrir d'un nombre croissant d'attaques (plus de 20 % l'année dernière), dans la mesure où l'activisme atteint depuis deux ans le monde des affaires et pas uniquement les institutions nationales. De surcroît, ce monde des affaires est concerné de plus en plus dans le bas du marché. Ainsi, 53 % de PME supplémentaires ont été touchées par rapport au référentiel de l'année dernière.

Au-delà de cette menace toujours grandissante en nature et en degré, la deuxième complexité est liée à la complexité de la surface de nos clients, avec le mouvement vers le cloud hybride, souverain. Ils sont confrontés à une complexité technique pour laquelle ils nous demandent des idées.

La troisième complexité est relative à la régulation. Le projet de loi touche Orange Cyberdéfense comme fournisseur essentiel en tant que société de services numériques. Pour nous, le coût d'adaptation n'est pas très important, puisque nous étions déjà très certifiés et en conformité avec la régulation nationale. En revanche, il offre une opportunité de continuer à accompagner, y compris les TPE PME qui seront concernées par NIS 2. Dans le cadre de sa transposition, la loi concerne moins les services numériques, puisque seulement trois articles nous concernent.

Globalement, dans le cadre de cette transposition, il conviendra de ne pas faire de surenchère pour demeurer compétitif, mais également de veiller à la simplification dans les décrets qui suivront. À titre d'exemple, se pose la question de la diversité de la mise en œuvre de NIS 2 dans l'ensemble de la géographie européenne, et même au-delà. Quand on dispose de systèmes extrêmement décentralisés dans l'Union européenne, ou dans nos systèmes *offshores*, quels seront les systèmes d'environnement en technologies de l'information (ITALIE) concernés ou non par la directive NIS 2 ? En fonction de la nature des réseaux, de notre chaîne

d'approvisionnement, de notre modèle opérationnel, de notre relation client, la gestion sera probablement complexe. En conséquence, il faudra être très attentif à la manière dont certains décrets seront rédigés.

De plus, il importe ne pas réinventer de nouvelles certifications ou de nouveaux processus de remontée d'informations des incidents. Il en existe déjà, autant les utiliser et maximiser ce qui a été mis en place par l'Anssi en matière de certification.

Mme Katuiscia Benloukil, vice-présidente communication de Tehtris. Tehtris est une société française à l'échelle internationale spécialisée aujourd'hui dans les solutions de cybersécurité pour détecter et neutraliser automatiquement, de manière autonome et en temps réel, le cyber espionnage et le cybersabotage.

Je partage les propos de mes confrères sur les enjeux de souveraineté, mais aussi l'importance de donner une obligation de moyens à toutes les entreprises. L'objectif de la directive NIS 2, qui reprend les mécanismes du RGPD, vise à rendre le cyberspace plus sûr, afin que chaque entreprise, petite, moyenne ou grande, puisse bénéficier d'une couverture cyber et se protéger des menaces qui évoluent. Aujourd'hui, nous constatons en effet une augmentation du volume des attaques, mais aussi de leur sophistication.

Ces attaques sont polymorphes et leurs variants changent très rapidement grâce aux techniques cyber utilisées, du côté des attaquants. Les entreprises doivent donc être soumises à une obligation de moyens, en matière de défense et de couverture cyber. En conséquence, ce texte de projet de loi rentre parfaitement dans le cadre mis en place actuellement en matière de régulation. Toutefois, cette transposition ne doit pas constituer une difficulté supplémentaire pour les entreprises.

M. Arnaud Dechoux, directeur des affaires publiques de Sekoia.io. Sekoia est une *scale-up*, une grande start-up d'une centaine de personnes implantée notamment à Paris et à Rennes, mais également dans différents pays européens. Nous sommes un éditeur de technologies *BtoB* dédiées à deux domaines de spécialisation. Il s'agit d'une part du renseignement d'intérêt cyber, produit par une vingtaine de chercheurs qui suivent les groupes d'attaquants, qu'ils soient cybercriminels ou des espions affiliés des États. À ce titre, Sekoia est partenaire d'Europol et coopère régulièrement avec les forces de l'ordre et la justice dans la lutte contre la cybercriminalité.

D'autre part, Sekoia développe une plateforme en mode SaaS (*Software as a Service*) à l'attention des centres d'opérations de sécurité (SOC) permettant de détecter les cybermenaces grâce au renseignement cyber et à l'intelligence artificielle (IA) et d'y répondre automatiquement. Cette solution, également décrite par l'acronyme XDR, vient s'imbriquer avec d'autres rubriques de sécurité, comme les logiciels de détection et de réponse aux *endpoints* (EDR) produits par exemple

par Airbus, des pare-feu et des sondes, pour assurer une supervision étendue du système d'information.

Cette solution est commercialisée auprès de grandes organisations qui sont matures en cybersécurité, mais aussi et surtout de manière indirecte, via un modèle *BtoB*, grâce à des partenariats avec des prestataires de services, comme Orange Cyberdéfense, qui utilisent notre technologie pour protéger leurs clients finaux qui sont constitués autant de grands groupes que de PME et de TPE. L'ambition consiste à démocratiser une cybersécurité de haute performance pour les petites entreprises ou administrations. À ce titre, Sekoia s'inscrit dans la chaîne d'approvisionnement de toutes ces entités qui seront soumises à NIS 2. Sur ces deux spécialités, nos concurrents sont quasi exclusivement des grands groupes américains ou israéliens.

En matière de conformité, Sekoia ne part pas de zéro. Nous avons misé pour l'instant sur des certifications reconnues internationalement, ISO 27001, PCI DSS dans le secteur des cartes de paiement, ou des labels comme Cybersecurity Made in Europe pour France Cybersecurity, labels déclaratifs, mais qui ont le mérite d'exister.

S'agissant du projet de loi actuellement en discussion devant votre commission spéciale, nous souhaitons également rappeler que la directive représente une avancée significative pour assurer un niveau élevé et commun de résilience dans l'ensemble de l'UE, qu'il s'agisse d'un enjeu de sécurité nationale, mais aussi de souveraineté.

Initialement, nous avons émis un doute sur le fait que Sekoia entre directement dans le périmètre des entreprises soumises à la NIS 2, peut-être en tant que fournisseur de services d'informatique en nuage, ce qui ferait de nous une entité importante. Ceci est probable, mais pas certain. Quoi qu'il en soit, en tant que membre de la chaîne d'approvisionnement de ces entités essentielles ou importantes, nous serons soumis indirectement aux mêmes obligations.

Pour Sekoia, les enjeux se joueront principalement au niveau réglementaire, avec les décrets et les arrêtés qui seront pris. Je pense notamment au référentiel des exigences techniques et organisationnelles, actuellement en préparation par l'Anssi.

À ce sujet, je souhaite mettre en avant trois points concernant ce projet de loi, certains étant portés par les associations dont Sekoia est membre, notamment l'Alliance pour la confiance numérique (ACN) et Hexatrust, que vous auditionnerez demain. Premièrement, le texte impose aux entités entrant dans son champ de renforcer leurs actions en matière de gestion des risques et de protection cyber. Ceci bénéficiera sans doute, premièrement, aux consultants, aux auditeurs et aux prestataires de services de proximité. Mais à ce stade, rien ne garantit qu'il en soit de même pour les équipements et les solutions, car le texte n'établit pas de préférence européenne. Au contraire, il nous apparaît que le risque est élevé aujourd'hui si les organisations privées comme publiques font appel en majorité à des solutions cyber non européennes, suivant la tendance actuelle.

Si tel était le cas, la directive et sa transposition ne feraient ainsi que renforcer leur dépendance à des acteurs extra-européens, à rebours de l'objectif d'accroître la souveraineté numérique française et européenne. À ce titre, le crédit d'impôt cyber bien ciblé constitue peut-être une piste de réflexion, peut-être un vœu pieux. Cependant, nous soutenons le vote au niveau européen d'un Buy European Tech Act ou d'un Small Business Act qui permettraient d'appuyer l'innovation en Europe grâce à la commande publique.

Deuxièmement, nous appelons à assurer autant que possible une proportionnalité et une application harmonisée de ces nouvelles obligations. Pour une start-up comme Sekoia, qui investit déjà dans des certifications comme ISO 27001, l'ajout de nouvelles obligations passant par des audits, des certifications ou des labels – pas nécessairement obligatoires, mais très fortement recommandés – auprès de consultants externes représenterait des coûts importants et ne ferait que renforcer la complexité à se déployer à l'international.

Troisièmement, une de nos propositions concernerait l'association continue des experts du secteur à la rédaction des textes réglementaires, par exemple en précisant que la mise à jour du référentiel de l'Anssi devra s'opérer en concertation avec les organisations professionnelles de la filière cyber française. L'idée porte ainsi sur un comité de suivi associant notamment les représentants de la filière, pour assurer la cohérence et l'efficacité du dispositif dans le temps. L'objectif consiste à mieux s'adapter à l'évolution rapide des cybermenaces, mais aussi des technologies de cybersécurité.

En synthèse, NIS 2 et sa transposition constituent une opportunité pour le tissu économique français et pour une start-up comme Sekoia. Nous espérons qu'elle sera également une opportunité en matière de souveraineté pour la filière cyber, qu'il s'agisse des services, mais aussi des solutions, et non un accroissement de la complexité qui ne bénéficiera certainement qu'aux grands éditeurs, notamment extra-européens.

M. Éric Bothorel, rapporteur général. Je fais partie de ceux qui souhaitent limiter toute surtransposition dans le contexte géopolitique actuel. Il ne s'agit pas d'empiler des textes réglementaires dans chaque pays, mais de faire émerger un écosystème et un cadre régulatoire au niveau européen aussi harmonieux et homogène que possible.

Ayant relu les auditions qui ont eu lieu au Sénat sur ce projet de loi, dont les vôtres, j'ai perçu à la fois la totale conviction de la nécessité de lutter contre les attaques, votre connaissance de l'accroissement du risque, mais aussi une forme de crainte face à un risque d'empilement entre les contraintes initiées par la loi d'orientation et de programmation du ministère de l'intérieur (Lopmi) et les questions actuelles autour de la résilience. L'exercice de la Lopmi a-t-il été si difficile pour vous, acteurs et opérateurs de la cyberdéfense ? Votre retour d'expérience pourrait peut-être nous éclairer.

Ensuite, la mise en œuvre de la LPM a contribué au développement d'une politique industrielle autour des schémas de qualification de services. Ces schémas ont permis d'accroître le niveau d'exigence, non seulement vis-à-vis des opérateurs d'importance vitale (OIV), mais surtout vis-à-vis des offreurs. Il me semble important de prendre cela en compte et de réfléchir à la mise en place d'une politique industrielle qui permette la construction d'une offre répondant aux besoins.

Or tel n'a pas été le cas de l'offre qui a été développée avec la Lopmi. Le cadre est probablement ici trop contraignant ; les enjeux liés à la sécurité tenant plus de la souveraineté que de la résilience. Cependant, il faut une politique qui garantisse une offre de qualité tout en permettant agilité et compétitivité. Avez-vous le sentiment que la simplification de ces dispositifs et leur remise à la vie civile constitueraient une piste ?

En ce qui concerne la politique industrielle de solutions cyber, il me semble que le comité stratégique de filière cyberdéfense est aujourd'hui quelque peu en sommeil. Me le confirmez-vous ? N'y a-t-il pas là une opportunité, par le passage au civil de tout ou partie de ce qui a été mis en œuvre pour la défense, de relancer ce comité stratégique ?

Nous sommes aussi à l'écoute de votre point de vue sur les exigences concernant les OIV et leurs filières nationales et européennes, ainsi que leurs sous-traitants. Certains estiment que le maillon le plus faible permet d'évaluer la force de résistance d'une chaîne. D'autres nous disent que les contraintes seraient trop fortes pour leurs filiales. Quel est votre point de vue ?

Mme Anne Le Hénanff, rapporteure. Je souhaiterais savoir si chacun d'entre vous est concerné par des dispositions du titre II du projet de loi ou du titre I^{er} qui transpose la directive sur les résiliences des entités critiques (REC). Si tel est le cas, dans quelle mesure ?

Les sénateurs ont procédé à une modification substantielle de certaines définitions qui vont dans le bon sens selon moi, notamment sur la partie concernant NIS 2. Va-t-elle assez loin ? Faut-il procéder à de plus amples clarifications ?

J'imagine également que certains d'entre vous seront concernés par le régime dérogatoire appliqué aux entités essentielles, aux entités importantes, aux administrations d'État, à leurs établissements publics administratifs qui exercent, entre autres, des activités dans le domaine de la sécurité publique, de la défense nationale ; et pour leurs réseaux et systèmes d'information prévus à l'article 14. Que pensez-vous de cette dérogation et de la rédaction de l'article ? Cette dérogation s'appliquerait-elle, le cas échéant, à l'ensemble de vos sous-traitants ?

M. Mickaël Bouloux, rapporteur. Je suis rapporteur du titre III du projet de loi, c'est-à-dire les articles qui concernent la transposition de la directive européenne sur la résilience opérationnelle numérique du secteur financier, dite Dora. Êtes-vous conduits à intervenir auprès des entités financières ? Comment

appréciez-vous leur maturité pour la cybersécurité ? Comment intervenez-vous dans ce domaine, le cas échéant ? Le secteur financier présente-t-il des spécificités par rapport à d'autres secteurs économiques ou industriels s'agissant des attaques et des menaces ?

M. Michaël Barthellemy. NIS 2 ne constitue pas un grand changement pour Airbus, dans la mesure où nous sommes déjà fortement réglementés, par la LPM ou NIS 1 notamment, d'autant plus que la France était en avance dans ce domaine par rapport aux autres pays européens.

En revanche, NIS 2 suscite une grande quantité de travail dans la démonstration de la preuve. Comme nous l'avons indiqué aux sénateurs, nous serions favorables à un label, un « tampon » que fournirait l'Anssi pour attester que nous avons bien répondu aux différentes contraintes, qui éviterait de devoir procéder à de nouveaux audits, qui sont à la charge de l'entreprise.

M. Arnaud Dechoux. Sekoia n'est pas concerné par la Lopmi ou des discussions spécifiques sur la défense ou les OIV. En revanche, je partage l'idée selon laquelle le maillon le plus faible constitue la bonne mesure de la résilience de la filière. Une start-up comme Sekoia, qui est productrice de solutions, s'inscrit dans la chaîne d'approvisionnement des entités qui seront soumises autant à REC et à NIS 2, qu'à Dora. De notre côté, l'attente portera sur les impacts contractuels de ces directives sur les entreprises concernées. En effet, les obligations qu'elles devront respecter auront également une répercussion à notre niveau, par exemple en termes de notification d'incidents.

Nous sommes également soumis à l'acte d'exécution pour NIS 2 qui a été publié l'été dernier et qui fournit de nombreux détails, par exemple les éléments constitutifs d'un incident et les délais associés en matière d'intervention.

Ensuite, les entités financières sont généralement plus matures en termes cyber, même si certains acteurs de la fintech devront monter en compétences. Très concrètement, Dora constitue une opportunité commerciale pour une entreprise comme la nôtre. Pour le renseignement cyber, les entités financières devront par exemple faire appel à des consultants pour passer des tests de résilience basés sur des menaces de type *Threat-Led Penetration Testing (*TLTP). Encore une fois, nous espérons que les acteurs européens ne seront pas oubliés ou du moins qu'ils pourront être promus par ce genre de dispositifs. Enfin, en matière de menaces spécifiques, je précise que les Nord-Coréens sont experts dans la conduite d'opérations lucratives ciblant notamment la finance.

M. Olivier Bonnet de Paillerets. Orange Cyberdéfense sera concerné au titre de la *supply chain* des entreprises qui devront répondre aux exigences de la directive Dora. Certains de nos clients européens dans le secteur financier, notamment allemands, nous ont ainsi fait part de leurs exigences. Il faudra donc procéder à une forme d'éducation pour éviter que Dora ne soit transposée

intégralement pour des organisations qui ne sont pas contraintes de se conformer totalement à cette réglementation.

Le secteur financier est de plus en plus mature. À titre d'illustration, il a connu une baisse de 20 % du nombre de victimes, l'année dernière en Europe. Le secteur est conscient des enjeux, notamment de souveraineté, et il est prêt à consentir des efforts financiers pour augmenter la certitude d'éviter un risque sur le réseau.

Je me garderais de formuler un avis définitif sur le comité stratégique, mais souhaite vous apporter un témoignage. Je reviens de San Francisco, où je suis allé rencontrer de grands fournisseurs américains. J'ai été marqué par l'accélération de l'innovation sur les capacités en GPU (*Graphics Processing Unit*), les agents IA et l'augmentation de l'intelligence des robots, grâce aux milliards de dollars qui ont été injectés dans le secteur. L'innovation figure bien au cœur de la proposition de valeur et je pense qu'il s'agit là de la réponse, y compris aux enjeux de souveraineté.

Compte tenu de la diffusion descendante de la menace, la chaîne d'approvisionnement revêtira une criticité encore plus marquée qu'auparavant pour les acteurs essentiels. Il convient donc d'accorder des investissements à la *supply chain*.

Enfin, en tant que prestataire numérique, nous sommes assez peu concernés par le projet de loi tel que vous le mentionnez. Je crois qu'il s'agit essentiellement de trois articles, dont l'article 14.

M. Vivien Mura, directeur des technologies d'Orange Cyberdéfense. Orange Cyberdéfense accompagne une grande partie de la chaîne de valeur du numérique sur les différentes mises en conformité concernant NIS, Dora et prochainement le Cyber Resilience Act. Nous observons une hétérogénéité dans la maturité des différents maillons de la chaîne d'approvisionnement, dans la compréhension de la menace qui est pourtant de plus en plus transverse. Les attaquants sont animés par des objectifs très lucratifs et cherchent à s'infiltrer là où les portes sont ouvertes. L'hétérogénéité se constate également dans la capacité à faire face à ces différentes menaces. Les PME sont très ciblées, mais toutes n'ont pas les moyens de se mettre en conformité, ni même d'apporter une réponse sécuritaire aux différents scénarios de menace.

Quoi qu'il en soit, il n'y a pas d'alternative : il faudra investir collectivement, de manière homogène au sein de l'écosystème européen si nous voulons relever le défi de la résilience. Cet investissement pourra d'ailleurs constituer un facteur de compétitivité s'il est mené à bon escient. Il doit s'accompagner effectivement d'une politique industrielle forte et de démarches pédagogiques pour expliquer le rapport entre les textes, mais aussi leur bien-fondé au regard des enjeux de sécurité. Certaines entreprises très matures le comprennent déjà, d'autres ont besoin de s'approprier ces textes pour pouvoir mener les actions correctement.

Il faut également améliorer la coopération entre le secteur public et le secteur privé, entre l'État et les tissus industriels, notamment être capable de déléguer davantage des missions d'intérêt public vers le secteur privé. En effet, de telles actions participent aussi à la compétitivité du secteur privé, des prestataires, des fournisseurs de solutions face à une concurrence qui est assez féroce. Enfin, la capacité à prendre des risques en matière d'investissement, notamment par des capitaux privés, dans des entreprises du numérique européennes sera clef. C'est aussi de cette manière que nous pourrons nous assurer d'une forme de résilience et de respect des valeurs européennes.

Mme Katuiscia Benloukil. Selon les chiffres d'Orange Cyberdéfense, environ 60 % à 70 % des attaques concernent les PME, tout simplement parce qu'elles sont les moins bien protégées. Le secteur de l'assurance oblige les entreprises, surtout les PME, à se protéger, à être couvertes en matière de cybertechnologie. Par exemple, une attaque par un rançongiciel ne sera peut-être pas prise en charge si la PME ne démontre pas qu'elle a tout mis en œuvre pour se protéger technologiquement.

Au même titre qu'Arnaud Dechoux, je suis intéressée par les obligations contractuelles qui pèseront sur les entreprises, c'est-à-dire l'obligation de moyens. Les PME sont inquiètes des attaques qu'elles reçoivent, mais s'interrogent aussi sur la manière de prioriser un budget et une superficie financière pour pouvoir se préparer d'un point de vue assurantiel et technologique à cette conformité.

M. le président Philippe Latombe. Certains d'entre vous ont évoqué la question des certifications, qui est revenue à plusieurs reprises lors des travaux sénatoriaux. Par exemple, les Belges ont adopté dans leur transposition la référence à un certain nombre de normes internationales. Lors de son audition, l'Anssi a indiqué qu'elle ne soutenait pas cette démarche. De votre côté, seriez-vous favorable à une transposition intégrant ce type de référence, de la même manière qu'en Belgique ?

M. Aurélien Lopez-Liguori (RN). Le gouvernement a publié il y a quelques jours une stratégie nationale pour la cybersécurité qui détaille en quatre piliers sa réponse, notamment celle du ministère de l'intérieur, face à la montée de la cybermenace. Mais elle ne mentionne à aucun moment la souveraineté, ni l'exclusion des entreprises étrangères des marchés sensibles, et encore moins une préférence nationale ou européenne dans les marchés publics. Elle n'évoque pas non plus une politique industrielle à long terme capable de faire émerger des géants français et européens face aux géants extra-européens.

Ces enjeux sont pourtant vitaux ; vous en êtes l'incarnation. En tant qu'entreprises françaises, vous êtes en effet des acteurs clés de notre cybersécurité nationale. Vous protégez des hôpitaux, des collectivités, des infrastructures vitales, et vous êtes en première ligne face à la cybermenace de notre pays. Il est donc de notre devoir de vous soutenir ; il y va de l'avenir de notre pays.

Comment pouvons-nous aujourd'hui vous aider à travers NIS 2, afin que les externalités positives, les retombées économiques générées puissent en premier lieu être récupérées par des acteurs français et européens ? Dans les certifications, faudrait-il insérer des critères d'immunité aux règles extraterritoriales, afin de vous favoriser ?

Mme Sabine Thillaye (Dem). Plusieurs d'entre vous nous ont invités à ne pas surtransposer. Il me semble que l'Allemagne a déjà transposé dans son droit national les directives européennes. Quelle est votre vision à ce propos ? Plus largement, regardez-vous la manière dont les autres États membres transposent ? Quels seront les points de vigilance pour nous permettre de garantir une concurrence loyale ?

M. Michaël Barthellemy. En réalité, dans leur transposition, les Belges ont effectué un copier-coller de l'ISO 27001. Cela ne me paraît pas nécessairement être une bonne approche, mais cette solution présente l'avantage de la rapidité. La Hongrie a également procédé à une transposition et a mis en place un système d'audit accordant une préférence nationale : l'audit doit être mené en Hongrie, par des sociétés hongroises, dûment autorisées par les autorités.

La « préférence nationale » est donc déjà mise en œuvre dans d'autres pays européens. C'est la raison pour laquelle nous souhaiterions que l'Anssi propose une forme de reconnaissance, un « tampon », sans qu'il soit forcément nécessaire de l'inscrire dans la loi. Cela permettrait, pendant une période donnée, d'être exempté de demandes d'audits complémentaires.

M. Vivien Mura. Je souhaite répondre à la proposition de M. Lopez-Liguori concernant l'intégration d'une immunité contre des lois à portée extraterritoriale dans des certifications. Comme tout autre risque cyber, les accès à ses propres données qui peuvent être jugés légitimes font partie de l'analyse de risque.

Ensuite, les différentes entités ont besoin d'être outillées pour pouvoir effectivement mettre en place ces protections si elles le jugent nécessaire. En ce sens, la certification de sécurité peut offrir ce moyen, en tout cas pour des niveaux élevés. Il revient donc aux autorités compétentes d'indiquer comment cela doit intervenir, plutôt à échelle européenne. En effet, comprendre comment il est possible de mettre en place des mesures de différentes natures contre ce type de risques et de menaces est compliqué. En outre, la démarche nécessite une forme d'expertise technique, juridique, organisationnelle. Enfin, la certification constitue probablement à ce titre l'un des meilleurs leviers.

M. Arnaud Dechoux. Je partage les propos de M. Barthellemy en matière de certification. Il faudrait sans doute établir un tableau d'équivalence clair entre ISO 27001 et les choix de la France.

Je n'ai pas lu les différents textes de transposition existant dans les autres pays de l'UE. Néanmoins, il conviendra sans doute de passer des accords de

reconnaissance mutuelle, qui me semblent très importants. J'étais d'ailleurs assez surpris que ces modalités n'aient pas été prévues dès le départ dans la directive.

S'agissant de la souveraineté et de la préférence européenne, nous n'avons pas envie de tomber dans un certain fatalisme. Une telle préférence est probablement difficile à introduire dans la loi en France, mais cela devra sans doute passer par des dispositifs au niveau européen, afin de soutenir les PME de l'UE. Elle devra également se manifester par la commande publique pour favoriser ces PME et l'innovation. Les Américains l'ont fait depuis longtemps ; cette démarche prendra plus de temps en Europe, mais nous devons agir de la sorte.

Mme Katuiscia Benloukil. La réflexion doit s'effectuer sur l'ensemble de la chaîne de la donnée, qui concerne non seulement nos offres de solutions technologiques de protection cyber, mais aussi les clouds souverains, qu'il faut privilégier. Je rappelle à ce titre que 80 % des logiciels utilisés aujourd'hui par les entreprises du monde entier sont américains. Il est ici question d'autonomie stratégique, dont les entreprises doivent aussi bénéficier.

Je rejoins donc les propos d'Arnaud Dechoux concernant la réglementation, la rédaction des textes de loi. Dans les commandes publiques, il est nécessaire de privilégier les éditeurs et les fournisseurs de solutions souveraines, qu'elles soient cloud ou cyber.

M. Aurélien Lopez-Liguori (RN). La position française concernant le projet de certification européenne pour les services de cloud (EUCS) risque de ne pas prévaloir. La présente transposition nous offre une occasion qui est peut-être historique. Ne faudrait-il pas trouver des solutions pour que l'effort, les externalités positives induites par NIS 2, profitent aux entreprises françaises et européennes ? Avez-vous des idées à partager dans ce domaine ? Je parlais de certification, mais peut-être existe-t-il également d'autres pistes.

M. le président Philippe Latombe. Faudrait-il profiter du texte pour adopter une définition du renseignement d'origine sources ouvertes (Osint) ? En effet, un certain nombre d'acteurs déplorent son absence et incitent le législateur à établir un cadre dans ce domaine. De son côté, l'Anssi nous a indiqué qu'elle ne voyait pas de raison particulière de légiférer sur le sujet. Qu'en pensez-vous ?

M. Éric Bothorel, rapporteur général. Je prolonge la question de M. Lopez-Liguori. Comment nous organisons-nous pour nous assurer que cette transposition se transforme en bienfaits pour l'écosystème cyber et non uniquement pour les cabinets d'avocats ou les sociétés de conseil qui ne manqueront pas de vendre des prestations de conformité ? Comment renforcer « l'équipe de France » du numérique, au-delà des effets d'aubaine dont profiteront certains ?

M. Michaël Barthellemy. À mon avis, il n'est pas nécessaire de formuler une définition de l'Osint. En revanche, lorsque nos chercheurs effectuent des recherches de failles lors de tests d'intrusion (*pentests*) il leur arrive de déceler des vulnérabilités *zero-day*. Lorsque nous entrons en relation avec le prestataire de la

solution pour l'en informer, une fois sur deux, il nous rétorque qu'il n'effectuera pas de modifications et peut même nous menacer d'une action en justice si nous les publions. Dans ce cas, nous bénéficions du support de l'Anssi, qui vérifie que le travail a été mené dans les règles, même si cela ne nous offre pas de couverture juridique. Pendant les six à neuf mois où nous discutons avec l'éditeur de la solution afin qu'il effectue une correction, la vulnérabilité est exploitable dans le monde entier.

De son côté, la Belgique a inscrit dans sa loi la protection de sa recherche sur les vulnérabilités. Cela n'est pas le cas en France, où nous pouvons subir une action en justice sur deux éléments : la propriété intellectuelle et les droits d'auteur. En effet, lorsque nous décompilons du code, nous revenons au code original, qui relève des droits d'auteur. En conséquence, nous souhaiterions que nos recherches puissent être protégées. Encore une fois, lorsque nous décelons une vulnérabilité, cela profite généralement à la communauté entière.

M. Thierry Racaud. Vous nous avez interrogés sur l'opportunité que peut présenter NIS 2. Les solutions et les produits de cybersécurité sont en très grande majorité américains, même s'il existe des solutions souveraines. Une filiale d'Airbus, Storm Shield, produit ainsi des solutions et des produits de cybersécurité qui sont estampillés par l'Anssi.

Ensuite, nous ne sommes pas en contact avec des cabinets d'avocats dans nos activités de conseil et d'audit auprès de la *supply chain* aéronautique. L'Anssi a mis en place cette labellisation de prestataire d'audit et de conseil à la cybersécurité (PACS). Des entreprises comme la nôtre, qui disposent de ce label, sont en mesure d'intervenir auprès des sociétés pour les auditer. Ce label fait foi et montre l'expertise de nos sociétés face à des concurrents qui pourraient venir de l'extérieur.

M. Vivien Mura. Je ne suis pas certain que la certification soit le bon levier pour activer la préférence européenne, si tant est que cela soit possible. En effet, il existe un problème de rapport et de nature entre l'objectif d'une certification – qui traite plutôt des aspects de sécurité – et les objectifs de politique industrielle, où il est possible d'agir dans le cadre du code des marchés publics, ou établir des préférences d'origine dans certains cas de figure, pour couvrir des usages sensibles.

De fait, la commande publique fait partie des leviers de politique industrielle les plus forts, comme nous pouvons le constater dans d'autres pays. En conséquence, il ne faut absolument pas négliger les autres leviers, bien plus évidents que ceux relevant purement de la sécurité.

M. le président Philippe Latombe. Monsieur Barthellemy, vous nous avez posé une question sur les *pentests*, que nous prenons en note, même si cet aspect est sans doute trop incident pour pouvoir être intégré dans le projet de loi.

M. Arnaud Dechoux. Le « label volontaire » a été ajouté à la loi. Il s'agit d'une avancée, mais le caractère volontaire doit être conservé en tant que tel : il ne

doit pas devenir obligatoire et entraîner *de facto* un recours à des consultants, qui constituerait un risque économique assez important pour les start-up.

M. Olivier Bonnet de Paillerets. Je partage ce point de vue. Certaines sociétés de conseil se précipitent sur ce créneau, car elles y voient des éléments de croissance très importants. Il faut donc être très attentif à ce sujet. Enfin, s'agissant de la commande publique, si nous sommes leaders en France et dans certains pays européens, nous sommes très peu présents dans l'administration française.

M. le président Philippe Latombe. Je vous remercie pour vos interventions. Nous ne savons pas encore quand ce texte sera étudié dans l'hémicycle, probablement en septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer dans notre réflexion et produire un texte le plus clair possible.

6. Table ronde réunissant des entreprises de télécommunications, mercredi 4 juin 2025 à 17 heures

Lors de sa deuxième réunion du mercredi 4 juin 2025, la commission spéciale a organisé une table ronde réunissant des entreprises de télécommunications.

M. le président Philippe Latombe. Mes chers collègues, nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde consacrée aux entreprises de télécommunications.

Le panorama de la cybermenace 2024 de l'Agence nationale de la sécurité des systèmes d'information illustre la diversité et la gravité des menaces qui pèsent, entre autres, sur ce secteur. Sont distinguées les menaces à visée lucrative, celles à finalité d'espionnage, et enfin celles visant à déstabiliser nos sociétés, dans lesquelles s'inscrivent les actes de sabotage. Ainsi, l'ANSSI a traité en 2024 la compromission et le chiffrement par le biais d'un rançongiciel d'une entité du secteur des télécommunications. Fait marquant de 2024, certaines rares attaques DDoS d'ampleur visant des infrastructures de télécommunications ont eu des conséquences importantes sur la disponibilité de services critiques.

L'ANSSI remarque également que le « ciblage d'opérateurs de télécommunications à des fins d'espionnage est intense ». Ces deux dernières années, l'ANSSI a ainsi traité plusieurs incidents affectant des entités du secteur des télécommunications en France à des fins d'espionnage.

Nous avons le plaisir d'accueillir pour la fédération française des télécoms (FFT) : M. Patrick Guyonneau, président de la commission sécurité de la FFT et directeur de la sécurité du groupe Orange, M. Matthieu Hennebo, directeur cybersécurité d'Altice France – responsable sécurité des systèmes d'information (RSSI) du groupe Altice France et M. Corentin Durand, responsable des affaires

publiques de Bouygues Telecom. Le groupe Iliad est représenté par M. Patrice Millecamps, directeur des obligations légales et Mme Ombeline Bartin, directrice des relations extérieures.

Madame, Messieurs, nous serons attentifs à vos retours sur les aspects du projet de loi qui vont concernent particulièrement, en particulier sur les points susceptibles de susciter des interrogations. Nous serons également à l'écoute de vos propositions concrètes pour renforcer la sécurité et la résilience du secteur des télécommunications.

M. Patrick Guyonneau, président de la commission sécurité de la FFT, directeur de la sécurité d'Orange France. Je vous remercie de nous donner l'occasion de nous exprimer sur un texte que nous avons déjà évoqué avec certains d'entre vous. Les opérateurs de télécom ont été diligents vis-à-vis des cybermenaces depuis longtemps, dans la mesure où les cyberattaques quotidiennes ont permis très tôt aux opérateurs d'apprendre à les détecter et à s'organiser pour les contrer. Nous n'avons pas attendu le projet de loi pour adopter des pratiques, des mesures très strictes et pertinentes en matière de cybersécurité en fonction des analyses de risque, notamment pour nos systèmes d'information les plus sensibles, dont les dysfonctionnements engendrent un impact transverse très important sur la continuité d'activité des opérateurs.

Ces mesures ont été renforcées par les contraintes ajoutées par le code de la défense après la loi de programmation militaire (LPM) de 2013. La plupart des opérateurs sont ainsi devenus des acteurs très régulés, différentes réglementations européennes et nationales s'imposant à nous. Ces liens étroits avec nos autorités de tutelle, en particulier l'Anssi, en témoignent et permettent aux opérateurs de délivrer à votre commission un certain nombre de messages tirés de nos expériences. Nous avons fortement conscience des menaces systémiques qui pèsent sur nous, comme sur de nombreux autres industriels ou opérateurs de services, mais aussi des menaces très ciblées.

L'actualité démontre malheureusement que les opérateurs sont fortement ciblés. Par ailleurs, nous savons que le risque zéro n'existe pas. En conséquence, nous souhaitons participer à cet effort commun de rehaussement du niveau de cybersécurité. J'ajoute deux arguments importants sur le soutien à cette démarche d'ensemble. D'abord, nous faisons appel à un grand nombre de sous-traitants ou de prestataires dont le niveau de cybersécurité est très hétérogène. Nous avons donc intérêt à ce qu'il s'améliore. Ensuite, en raison de leur longue expérience, tous les opérateurs de télécommunication ont en général développé une forme d'activité *BtoB* dans ces domaines.

En revanche, lors de notre audition devant la commission supérieure du numérique et des postes (CSNP), représentée ici par Mme la députée Le Hénanff, mais aussi au Sénat, nous nous étions inquiétés d'une surtransposition législative, au sens d'une transposition maximaliste par le haut. Dans la première version du texte, les difficultés d'interprétation pouvaient être sources d'insécurité juridique.

Cette surtransposition aurait conduit à porter atteinte à la compétitivité des entreprises françaises et, *in fine*, à l'objectif d'harmonisation européenne. Nous remercions la CSNP et le Sénat d'avoir accepté un certain nombre d'amendements qui vont dans le bon sens selon nous.

Aujourd'hui, nous voudrions vous alerter sur l'une des principales questions posées aujourd'hui par ce projet de loi. Elle n'est d'ailleurs pas directement dans la loi, mais d'ordre réglementaire. Il s'agit du référentiel de mesures de cybersécurité, qui sera publié par l'Anssi. Ce référentiel, et notamment les règles prévues par l'article 14, n'est pas forcément utile pour tous les systèmes d'information de nos entreprises. Si notre cœur d'activité mérite sans doute de disposer d'un référentiel de haut niveau, toute la complexité ne peut pas être portée par l'ensemble des systèmes d'information.

Le texte de l'Anssi n'exige une conformité que pour les objectifs à respecter, mais en cas de contentieux avec nos clients, la difficulté réside pour nous dans cet objectif de résultat, potentiellement source d'une grande incertitude quant à sa portée et sa valeur. De plus, le principe de proportionnalité mis en avant par le directeur général de l'Anssi lors de son audition devant votre commission n'est pas encore suffisamment inscrit dans la loi à notre sens, malgré l'amendement sénatorial sur l'article 14.

Le changement d'échelle, avec l'assujettissement de NIS 2 à tous les systèmes d'information (SI), quelle que soit leur criticité, est problématique et nous semble contraire au principe de proportionnalité : toutes les activités des opérateurs ne peuvent être placées au même niveau de résilience.

Normalement, des analyses doivent être conduites par l'État et être transcrites dans une directive nationale de sécurité pour chaque secteur d'activité, pour nous permettre d'orienter nos efforts et nous focaliser là où ils sont le plus nécessaires. Le principe de mise en œuvre pour tous les niveaux d'exigence technique ne doit pas seulement s'appliquer sur les types d'entités. Ce n'est pas tant la taille de l'entité qui importe, mais la sensibilité des SI et l'impact en cas de dysfonctionnement.

Ensuite, la plupart d'entre nous sommes présents dans plusieurs pays européens. Nous avons ainsi pu constater comment d'autres pays ont transposé la directive NIS 2, laissant le soin aux acteurs d'apprécier leurs besoins par des analyses de risque et d'adopter des mesures strictement nécessaires en co-construction avec les autorités de tutelle. Il est hors de notre portée de réaliser pour l'ensemble de nos systèmes d'information des audits obligatoires, de déployer les mesures les plus complexes, comme des réseaux spécifiques d'administration, des postes spécifiques pour les administrateurs. Ce sont ces questions de mise en conformité qui nous posent problème, surtout dans des délais extrêmement réduits, puisqu'ils sont de l'ordre de trois ans. L'application des mesures les plus strictes occasionnerait environ 20 % de surcoûts pour un SI, à la fois dans la conception, mais aussi dans le maintien en condition quotidienne. Or nous avons déjà consenti

des investissements massifs pour d'autres raisons et notre secteur connaît actuellement une situation économique difficile.

Ensuite, nous nous interrogeons sur le niveau de sévérité des incidents à déclarer, dans la mesure où tout incident cyber est susceptible d'engendrer de grandes conséquences. Il est donc difficile pour nous de cerner exactement ce que nous devrons signaler à l'Anssi, dans des délais très contraints, qui ne nous permettront pas de conduire des analyses d'impact suffisantes.

Nos principales recommandations reposent sur une priorisation et une hiérarchisation dans un souci de proportionnalité des exigences, afin d'éviter la congestion et des surcoûts. Nous souhaitons également échelonner dans le temps la mise en œuvre de ces mesures techniques ou organisationnelles. Ensuite, des mises en œuvre d'accords de reconnaissance mutuelle permettraient aux organisations de satisfaire aux exigences de l'Anssi dans plusieurs États membres qui se contentent d'une conformité à ISO 27000.

S'agissant des incidents importants, nous souhaiterions que des critères plus précis soient établis avant d'enclencher une notification, sous peine d'engorger le système de l'Anssi. Nous estimons également qu'un organe de supervision parlementaire sur la mise en œuvre de ces règles NIS 2 pourrait représenter une bonne solution, afin d'éviter une surtransposition uniquement administrative.

Malgré la qualification par l'Anssi de notre secteur comme « supercritique », les pouvoirs publics n'ont pas pour l'instant classé les télécoms au rang de services essentiels dans notre pays, notamment dans l'arrêté du 5 juillet 1990, fixant les consignes générales de délestage des réseaux électriques. Le rapporteur Éric Bothorel rappelait à juste titre lors de l'audition du secrétariat général pour la défense et la sécurité nationale (SGDSN) l'importance des systèmes de télécommunication pour la résilience de l'ensemble des entités.

M. Matthieu Hennebo, directeur cybersécurité d'Altice France. La notion de proportionnalité concerne les mesures de sécurité que nous pourrions être conduits à identifier et à devoir mettre en œuvre sur ces systèmes en fonction de la criticité des services qu'ils délivrent. La proportionnalité porte également sur leur délimitation dans le cadre de la mise en œuvre des mesures de cybersécurité.

M. Corentin Durand, responsable des affaires publiques de Bouygues Telecom. Je partage les propos du président de la commission sécurité de la FFT et me permets d'insister une nouvelle fois sur les notions de priorisation et de proportionnalité.

Aujourd'hui, un opérateur comme Bouygues Télécom opère sur des milliers de systèmes d'information, des services qui sont essentiels, aussi bien pour les citoyens que pour les entreprises avec lesquelles nous travaillons. Ces systèmes d'information doivent être robustes et évidemment protégés. Cependant, les systèmes d'information sur lesquels nous opérons aujourd'hui ne peuvent pas tous être considérés comme critiques.

Dans notre entreprise, nous avons défini une forme de nomenclature de sensibilité des applications et systèmes d'information avec lesquelles nous travaillons quotidiennement pour les activités que nous gérons, c'est-à-dire des activités réseaux généralement critiques, ou des activités indépendantes des activités réseaux, sur lesquelles la compromission n'aura pas du tout le même impact.

Il existe quatre typologies de sensibilité. Un certain nombre de systèmes d'information sont non-sensibles, puisque leur compromission ne provoquerait pas de problèmes graves ou alors modérés et qui ne remettraient pas nécessairement en question notre activité ou des activités qui existent grâce à nous.

En revanche, sur deux niveaux de sensibilité élevés, voire très sensibles, les règles les plus strictes doivent s'appliquer, y compris les analyses de risque qui nous paraissent absolument essentielles sur ces types de systèmes d'information, mais qui ne provoqueraient pas de problèmes graves, disproportionnés, en cas de compromission. C'est la raison pour laquelle nous parlons effectivement de proportionnalité jusqu'à présent, en sachant que la proportion de systèmes d'information que nous pourrions considérer comme sensibles et très sensibles est plutôt limitée et que de nombreuses applications aux SI ne rentrent pas dans ces deux catégories.

Patrick Guyonneau a évoqué le sujet de la qualification des opérateurs télécoms comme des services prioritaires. Lors de l'hiver 2022-2023, voire de l'hiver 2023-2024 dans une moindre mesure, nous avons ainsi été quelque peu surpris d'apprendre que nos infrastructures pourraient potentiellement faire l'objet de délestages électriques, non seulement parce que nous sommes aussi dans l'obligation d'assurer en permanence l'acheminement de nos communications d'urgence – une activité absolument essentielle – mais aussi parce que les infrastructures télécoms sont absolument incontournables.

Le deuxième élément de cette priorisation concerne la réaction qui devrait être la nôtre à l'occasion d'incidents climatiques. Nous en avons connu un certain nombre récemment et nous serons probablement conduits à en connaître de plus en plus. Dans ces circonstances, certaines de nos antennes finissent par ne plus fonctionner, parce qu'elles subissent une rupture d'alimentation électrique. Il s'agit non seulement de sécuriser nos antennes et le réseau électrique, mais surtout de nous assurer que ces infrastructures soient de nouveau alimentées dès le déploiement de la réponse de crise. Nous estimons qu'il faut effectivement relever le niveau de sécurisation des infrastructures supercritiques.

Mme Ombeline Bartin, directrice des relations extérieures d'Iliad-Free. Je partage l'ensemble des préoccupations qui ont pu être soulignées par la FFT et les différents opérateurs. En synthèse, ce texte comporte trois enjeux principaux pour nous.

En premier lieu, il faut nous laisser le temps de la mise en œuvre du texte. Le directeur général de l'Anssi avait évoqué trois ans, ce qui constitue une durée minimale. En effet, si les opérateurs entreprennent depuis plusieurs années des mesures d'audit, de prévention et de sécurisation de leurs SI, le texte de transposition nous fait changer d'échelle. En conséquence, il serait plus sécurisant pour nous que la loi inscrive un délai de mise en œuvre, comme cela peut être le cas pour d'autres dispositions du texte.

Deuxièmement, toute surtransposition engendrerait pour nous des complexités et des coûts supplémentaires. Or, la mise en conformité avec ce nouveau texte de l'ensemble de nos SI sera déjà assez coûteuse.

Troisièmement, le projet de loi prévoit de nombreux renvois à des décrets sur des points substantiels, notamment le référentiel ou des procédures de notification. Ces recours constituent pour nous une source d'insécurité ; nous préférerions savoir dès le départ les règles que nous devrons appliquer, les procédures que nous devrons respecter. Nous préconisons donc de simplifier le plus possible le recours à ces décrets.

Un autre point d'attention est lié au référentiel évoqué à l'article 14. La définition de ce référentiel représentera un enjeu considérable pour nous, d'autant plus qu'aujourd'hui, la norme ISO 27001 prévoit des procédures que nous respectons d'ores et déjà. Enfin, le dernier élément concerne l'article 17. Il serait sécurisant de déterminer un point unique de notification des incidents et des vulnérabilités. À l'heure actuelle, il existe en effet une multiplicité de procédures entre Bercy, le ministère de l'intérieur et l'Anssi.

En conclusion, je souligne que la rédaction par le Sénat porte également des avancées, notamment la reprise des définitions des incidents et des vulnérabilités et la précision des délais de la procédure graduée prévue par la directive. Nous demandons à l'Assemblée nationale de conserver ces points qui offrent une meilleure visibilité et une meilleure définition de l'objet des procédures impliquées.

M. Éric Bothorel, rapporteur général. Madame Bartin, vous venez d'évoquer votre attachement à un délai de mise en œuvre. Je me permets de souligner que vous avez déjà gagné un an, puisque nous examinons un texte qui aurait dû être adopté l'année dernière. Même si la version définitive du texte n'est pas stabilisée, ses grandes lignes sont connues de longue date, me semble-t-il.

Parmi les priorités 2022-2027 des opérateurs télécoms présentées par la FTT, la proposition n° 2 vise à « *intensifier la prévention et la lutte contre les actes de malveillance et de dégradation des infrastructures numériques en renforçant les réquisitions en diversifiant les sanctions pénales à l'encontre de leurs auteurs* ». La proposition n° 6 consiste à « *évaluer la conformité, d'une part des actes législatifs existants, et d'autre part de toute réforme, au principe de concurrence équitable (*level playing field*) avec les autres acteurs du numérique afin de ne plus créer de nouveaux écarts entre les acteurs, généraliser les études d'impact ex ante et ex post*

sur ces sujets ». La proposition n° 7 a pour objet de *« poursuivre les travaux de réforme de la directive NIS afin que les éditeurs de logiciels d'importance stratégique et les équipementiers soient responsabilisés au même titre que les opérateurs télécoms* ».

La multiplication du nombre d'acteurs concernés par les directives NIS 2 et REC est patente, y compris le secteur public. Vous avez développé selon vos propres termes une sécurité robuste en faveur de la résilience de l'intégralité de la chaîne de valeur. Or nous entendons qu'il faudrait être plus souple avec les filiales, tout en étant plus exigeant avec les sous-traitants. Quel est votre point de vue à ce sujet ?

Ensuite, vous êtes des entreprises de télécoms, mais une partie des réseaux sont sous statut public. Le Sénat semble attentif à ce que le projet de loi n'ait pas un impact trop fort les collectivités. Qu'en pensez-vous ? Enfin, les asymétries réglementaires entre opérateurs télécoms et géants d'internet perdurent. Vous nous avez régulièrement interpellés afin qu'elles soient impérativement corrigées pour assurer un traitement équitable de tous les acteurs de l'écosystème numérique. Pensez-vous que les dispositions de ce projet de loi puissent y contribuer ?

Mme Anne Le Hénanff, rapporteure. Les modifications apportées par le Sénat à ce stade vous conviennent-elles ? Faut-il préciser encore plus quelques notions ?

Ensuite, les procédures en matière de gestion de crise sont-elles spécifiques à chacune de vos entreprises ou existe-t-il un référentiel commun, par exemple sous l'égide de la FFT ? Comment vous inscrivez-vous dans des procédures telles que les plans communaux, départementaux ou préfectoraux de sauvegarde ? Le texte doit-il approfondir la gestion de crise et des moyens à mettre en œuvre pour vous guider ? Ce texte vous conduira-t-il à faire évoluer vos procédures collectives ou individuelles ?

Enfin, M. Guyonneau, vous avez souligné l'importance à vos yeux de l'idée de proportionnalité, en fonction de la taille des opérateurs. Pourriez-vous nous fournir des exemples précis ? Quels risques distinguent un petit opérateur télécom d'un opérateur de plus grande taille ?

M. Patrick Guyonneau. Chaque opérateur dispose de ses propres procédures de gestion de crise, pour différentes raisons. Cependant, nous avons fortement travaillé sur nos procédures avec l'État, en particulier le commissariat aux communications électroniques de défense (CCED) et le centre opérationnel de gestion interministérielle des crises (Cogic). Nous avons ainsi produit des efforts, qui ont été salués, sur la rapidité de prévention et l'impact estimé de tel ou tel incident. En conséquence, il ne semble pas nécessaire que la loi apporte des compléments à ce sujet.

Par ailleurs, nous échangeons en temps réel entre opérateurs, dès que l'un d'entre nous souffre d'un incident. Les Jeux olympiques, qui se sont déroulés avec

succès, ont d'ailleurs prouvé la validité de nos procédures face aux incidents qui se sont produits. En revanche, comme le soulignait Mme Ombeline Bartin, nous sommes demandeurs d'un interlocuteur unique dans le cadre du signalement des incidents.

Je ne pense pas que la taille des opérateurs soit l'élément le plus discriminant. Cela dépend de leur place dans le service que l'État juge essentiel ou critique pour la résilience de la société. Un petit opérateur peut être fondamental dans le transport de la donnée, par exemple sur une zone très particulière. À ce sujet, et pour répondre à une question du rapporteur Bothorel, tout n'est pas réglé vis-à-vis des sous-traitants ou des concurrents. Pour l'instant, un certain nombre de partenaires industriels, ne sont pas forcément visés dans cette chaîne, lorsque l'on réfléchit à la résilience de bout en bout.

Enfin, je précise que nous conduisons des exercices réguliers avec les différents organismes de l'État.

M. le président Philippe Latombe. S'agissant de la directive sur la résilience opérationnelle numérique du secteur financier (Dora), avez-vous d'autres points à apporter à notre connaissance concernant le titre III ?

M. Matthieu Hennebo. Les opérateurs télécom délivrent des prestations et des services à de nombreuses entreprises du secteur bancaire et assurantiel. À ce titre, une source d'inquiétude concerne la capacité qui sera laissée à ces clients de pouvoir opérer des audits assez larges, dans le cadre de Dora.

Nous souhaiterions obtenir plus de lisibilité sur l'encadrement applicable à ces échanges qui, rappelons-le, restent d'ordre commercial. Il s'agirait d'obtenir des précisions sur les systèmes à auditer, leur périmètre ; mais également le niveau d'accès aux informations accordé. En effet, si le service est effectivement « sensible », faudra-t-il donner l'accès à des informations très sensibles ? Il s'agit là d'un point de vigilance sur l'application et la transposition de Dora, mais aussi les contractualisations qui en découleront.

M. Corentin Durand. Dora placera au centre du jeu de nouvelles autorités de régulation du secteur financier, en toute logique. Je partage à ce titre les propos du directeur de l'Anssi, quand il indique que son agence ne doit pas être exclue de l'application de ce règlement. En effet, nous serons concernés par les audits potentiels et avons besoin que l'autorité de tutelle avec laquelle nous avons l'habitude de travailler soit concernée, au titre de la réponse aux incidents ou tout simplement pour le suivi de l'interfaçage entre les réglementations NIS 2 et Dora.

M. le rapporteur général Bothorel, nous n'avons pas à ce jour d'avis sur les obligations des collectivités. Cependant, étant confrontés à la même problématique, nous constatons que la marche demeure assez haute. J'en profite également pour souligner les actions des opérateurs en matière de développement d'offres de diagnostic et de programmes de mise en conformité qui s'adressent non seulement aux nouvelles entités qui seront assujetties à NIS 2, mais aussi aux collectivités. Si

ces dernières ressentent le besoin d'être accompagnées, nous nous tiendrons à leur disposition.

M. le président Philippe Latombe. Si je comprends bien, deux questions se posent pour vous dans le cadre de Dora. La première concerne les audits et votre assujettissement à l'Autorité des marchés financiers (AMF) et à l'Autorité de contrôle prudentiel et de résolution (ACPR), ce qui n'était pas le cas auparavant, puisque l'Anssi était votre seul interlocuteur.

La deuxième est liée à la faculté des sociétés soumises à Dora d'auditer les entreprises avec lesquelles elles travaillent, dans un cadre contractuel. Vous redoutez que ces sociétés vous imposent des audits réguliers, potentiellement sur des systèmes d'information qui ne les concernent pas, mais qu'il pourrait être important pour vous de conserver à titre confidentiel ou, à tout le moins, de ne pas trop les exposer. Ai-je bien résumé la situation ?

M. Matthieu Hennebo. Exactement. Il s'agit de bien recentrer cette notion d'audit et la sensibilité de certains systèmes et services qui pouvaient être délivrés. Aujourd'hui, la criticité ne porte pas sur le service à proprement parler, mais sur l'opérateur. Il faudrait donc opérer un cadrage, notamment au niveau du service qui est concrètement mis à disposition du client bancaire. Simultanément, l'Anssi devrait être en mesure d'arbitrer la notion d'audit ou la capacité à pouvoir donner accès à certaines informations de systèmes sensibles.

Notre interrogation porte donc sur les critères selon lesquels un opérateur sera jugé critique par une banque. S'agira-t-il de son service ? La catégorisation sera-t-elle établie par une autorité européenne ou nationale de surveillance, en l'occurrence l'AMF ou l'ACPR ?

M. le président Philippe Latombe. Identifiez-vous dans le texte des éléments sur lesquels il faudrait apporter des précisions et, si tel est le cas, lesquelles seraient-elles ? En effet, selon que la loi se concentre sur la notion de service ou d'opérateur, les champs sont totalement différents. Nous devons absolument éviter les effets de bord, d'autant plus qu'il s'agit d'une transposition et non uniquement d'une loi d'initiative française.

M. Corentin Durand. À ce stade, il s'agit surtout pour nous d'une alerte, que nous n'avions pas initialement identifiée sur ce texte. Je ne suis pas certain que la réponse à la question de la criticité des services de connectivité doive être d'ordre législatif, compte tenu de la technicité des sujets. En revanche, ce sujet ne doit pas être oublié et nous espérons pouvoir le retravailler. Au-delà, il nous semble essentiel que notre autorité de tutelle habituelle, l'Anssi, puisse être réellement impliquée dans la mise en œuvre de Dora. Cela nous faciliterait la tâche.

M. Éric Bothorel, rapporteur général. Madame Bartin, qu'entendez-vous par « simplifier le recours aux décrets » ? Faut-il inscrire dans le droit le référentiel ou la procédure de notification ? J'aimerais obtenir des éclaircissements sur cet aspect.

M. le président Philippe Latombe. Je prolonge la question du rapporteur général. Les précisions que vous avez évoquées concernant Dora devraient-elles être inscrites dans la loi ? *A priori*, cela relèverait plutôt du domaine du réglementaire, mais dans vos propos liminaires, vous indiquiez votre souhait de voir la partie réglementaire limitée.

Ces aspects n'avaient pas été mentionnés lors des auditions du Sénat. Or nous intervenons dans le cadre d'une procédure accélérée et nous allons devoir nous accorder avec les sénateurs. Cela implique de parvenir à une écriture la plus précise possible, afin de faciliter le travail de la commission mixte paritaire (CMP). Mes demandes de précision ont pour objet de permettre aux sénateurs d'y réfléchir de leur côté, avant la CMP.

Mme Ombeline Bartin. Certaines mesures ne peuvent effectivement être définies que par voie réglementaire. Simplement, nous souhaitons pouvoir les anticiper au maximum, ce qui n'est pas le cas aujourd'hui. S'agissant du référentiel, nous souhaitons nous assurer qu'il correspondra bien à la norme ISO 27 001.

Les procédures de notification sont assez bien définies dans le texte de loi et dans la directive. En conséquence, nous nous demandons quelles précisions pourraient être apportées par voie réglementaire, dans la mesure où les procédures en vigueur aujourd'hui fonctionnent et ont fait leur preuve.

M. le président Philippe Latombe. Si je comprends bien, vous seriez favorable à une démarche similaire à celle employée par les Belges, c'est-à-dire transposer en faisant immédiatement référence à ISO 27001, plutôt que d'établir un autre référentiel.

Mme Ombeline Bartin. Oui.

M. Patrick Guyonneau. D'une certaine manière, oui. À tout le moins, nous souhaiterions qu'il existe des équivalences, telles que celles mentionnées par l'Anssi. Ainsi, le respect de l'ISO 27001 offrirait une présomption de conformité. Cette question rejoint celle de la proportionnalité dans les services rendus. En effet, les systèmes d'information se comptent par milliers et n'ont pas tous le même degré d'importance ni de sensibilité. C'est la raison pour laquelle, avant de parvenir au référentiel de l'Anssi, il est nécessaire de disposer d'un décret qui précise cette proportionnalité par rapport à la criticité du service rendu.

Il s'agit d'éviter des situations rocambolesques pour tous les opérateurs paneuropéens. Par exemple, notre filiale belge *BtoB* pourrait travailler en France grâce à une présomption forte de compatibilité NIS parce qu'elle est ISO 27001 en Belgique, quand cela ne serait pas le cas d'Orange Business France, qui n'aurait pas encore intégralement coché toutes les cases du référentiel Anssi. Le problème porte bien sur la gestion de la cohérence.

Ensuite, les articles 14 et 17 posent question, en particulier sur les pertes financières. Nous ne sommes pas en mesure d'évaluer la matérialité des impacts

financiers pour un certain nombre de clients. Plus précisément, il s'agit de l'alinéa 3 de l'article 17. Selon nous, il mériterait sans doute d'être rédigé différemment et plutôt parler de l'impact sur le service. La résilience n'équivaut pas à un risque zéro, mais concerne la continuité de service. À titre d'illustration, en cas de crise, l'accès à internet n'a pas la même importance selon qu'il s'agit d'un particulier ou d'un hôpital.

Une question du même ordre se pose à l'article 14, concernant les conséquences économiques et sociales. En gestion de crise, lorsqu'un incident survient, et compte tenu des délais imposés pour effectuer les déclarations, nous sommes incapables de nous occuper des conséquences économiques et sociales. Dans de telles circonstances, notre principale préoccupation consiste à rétablir le service, avec une priorité accordée aux numéros d'urgence.

En résumé, il conviendrait de clarifier ce qui est considéré comme « essentiel » dans les articles 14 et 17 ou, à tout le moins, renvoyer à un premier décret. En effet, je ne partage pas l'idée selon laquelle nous aurions le temps pour la mise en application. De fait, les délais courent depuis le 17 octobre de l'année de la publication de la directive. Pour certains sujets, le chronomètre est déjà enclenché, mais nous ne savons pas ce que nous devons faire.

M. Éric Bothorel, rapporteur général. Quel est votre point de vue concernant la sanction pénale des dirigeants ?

M. Patrick Guyonneau. Ici aussi, il existe un enjeu d'harmonisation et de cohérence, puisque le texte ne prévoit pas de sanction pénale pour un haut fonctionnaire qui n'aurait pas agi comme il le devait en matière de systèmes d'information. En effet, certaines données des ministères sont plus sensibles que celles que nous détenons. Soyez rassurés, chez tous les opérateurs, les sujets de sécurité sont extrêmement importants. Nos comités exécutifs les abordent et les font figurer au rang des priorités lors des analyses de risques.

M. Corentin Durand. Le secteur des télécoms est extrêmement régulé et il existe déjà de nombreux textes qui prévoient d'engager la responsabilité des dirigeants en cas de non-respect des obligations qui leur incombent. Je partage le point de vue de M. Guyonneau : les enjeux cyber figurent parmi les priorités, au quotidien.

M. le président Philippe Latombe. Nous avons évoqué la problématique de Dora et la question de l'assujettissement indirect. Existe-t-il des zones de frottement, des incompatibilités, entre NIS 2 et la directive REC vous concernant ? Entre le texte de loi et d'autres réglementations comme le règlement général sur la protection des données (RGPD), par exemple ?

M. Patrick Guyonneau. Non, pas à ma connaissance, hormis le sujet du *non bis in idem* ; nous ne voulons pas être punis deux fois. Ensuite, un incident peut engendrer de multiples conséquences. En fonction du type de conséquence,

plusieurs personnes doivent être alertées et nous sommes préoccupés à l'idée d'en oublier une.

S'agissant de Dora, la plupart des clients bancaires ne réalisent pas eux-mêmes les audits, mais font appel à des cabinets ou des prestataires extérieurs. À ce titre, nous ne souhaitons pas devoir multiplier les audits, *a fortiori* avec des acteurs qui ne seraient pas forcément nationaux ou européens.

M. le président Philippe Latombe. Considérez-vous que le sujet du *non bis in idem* est aujourd'hui traité dans le texte issu du Sénat ?

M. Patrick Guyonneau. Il me semble que cet aspect a été clairement traité par M. Strubel, qui a indiqué qu'il n'y aurait pas de double sanction. Nous estimons que vous envisagerez cet aspect avec sagesse, dans le texte.

M. Éric Bothorel, rapporteur général. Avez-vous identifié des points de frottement entre le projet de loi tel qu'il a été rédigé par le Sénat et d'éventuelles dispositions du règlement européen sur la cyberrésilience (Cyber Resilience Act, CRA) ?

M. Patrick Guyonneau. Il est encore un peu trop tôt pour nous prononcer à ce sujet, nous sommes en train d'étudier le CRA, qui porte des sujets importants vis-à-vis d'un certain nombre de nos équipements.

M. le président Philippe Latombe. Si vous identifiez rapidement des éléments, nous vous serions reconnaissants de nous en faire part, afin que nous puissions anticiper au maximum d'éventuels frottements, à plus forte raison si le texte est examiné en septembre dans l'hémicycle.

M. Matthieu Hennebo. S'agissant de Dora, je souscris aux propos de M. Guyonneau concernant l'accès d'auditeurs étrangers à des informations sensibles. Un opérateur pourra être soumis à Dora dans la mesure où il délivre des services à une banque ou une assurance. Sans entrer dans des considérations très techniques et complexes qu'il n'est pas envisageable d'intégrer dans la loi, nous souhaiterions bénéficier de suffisamment de visibilité, de cohérence. Par exemple, il serait utile que l'Anssi puisse à un moment donné se prononcer pour confirmer qu'un service délivré par l'opérateur pour la banque dans tel ou tel contexte est critique ou non.

M. le président Philippe Latombe. Je vous remercie. Nous ne savons pas encore quand ce texte sera étudié dans l'hémicycle. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer dans notre réflexion et produire un texte le plus clair possible. L'objectif consiste en effet à éviter des zones d'ombre, des effets de bord.

7. Table ronde réunissant des experts de la cybersécurité, jeudi 5 juin 2025 à 9 heures 30

Lors de sa première réunion du jeudi 5 juin 2025, la commission spéciale a organisé une table ronde réunissant des experts de la cybersécurité : CyberTaskForce : M. Sébastien Garnault, fondateur, M. Philippe Luc, co-fondateur de Anozr Way et Mme Anne-Elise Jolicard, responsable des affaires publiques ; Clusif : Mme Florence Puybareau, directrice, M. Benjamin Leroux, administrateur, Mme Garance Mathias, administratrice, et Mme Eva Aspe, en charge des affaires publiques ; Hexatrust : M. Jean Noël de Galzain, président, Mme Dorothée Decrop, déléguée générale et Mme Sara Durand, consultante ; CyberCercle : Mme Bénédicte Pilliet, présidente, MM. Christian Daviot et François Coupez, senior advisors ; CESIN : Mme Mylène Jarossay, vice-présidente, et M. Arnaud Martin, vice-président ; Alliance pour la confiance numérique (ACN).

M. le président Philippe Latombe. Mes chers collègues, nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde rassemblant des spécialistes de la cybersécurité. CyberTaskForce est représenté par son fondateur Sébastien Garnault, Philippe Luc, membre de Cyber Task Force et président d'Anozr Way, ainsi que par Anne-Élise Jolicard, responsable des affaires publiques d'Anozr Way. Nous recevons également les représentants de CyberCercle : Bénédicte Pilliet, sa présidente, ainsi que Christian Daviot, François Coupez, Stéphane Meynet, tous trois *senior advisors*. Le Clusif est représenté par trois administrateurs, Benjamin Leroux, Michel Dubois et Garance Mathias ; Hexatrust par son président Jean-Noël de Galzain et sa déléguée générale Dorothée Decrop. Enfin, nous accueillons Daniel Le Coguic, président de l'Alliance pour la confiance numérique (ACN) accompagné du directeur général Yoann Kassianides ; ainsi que les vice-présidents du club des experts de la sécurité de l'information et du numérique (Cesin), Mme Mylène Jarossay et M. Arnaud Martin.

La France bénéficie d'un écosystème dynamique et structuré dans le domaine de la cybersécurité, à la fois grâce à ses entreprises qui conçoivent et développent des solutions innovantes et à ses associations qui œuvrent activement à la sensibilisation des acteurs économiques face aux risques cyber.

À ce titre, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a par exemple organisé le 17 février dernier au Campus Cyber un exercice grandeur nature de gestion de crise. Cette initiative a permis de renforcer la coordination des différents acteurs et d'enrichir notre culture de réponse face aux menaces émergentes. Le projet de loi que la commission spéciale est chargée d'examiner vise à renforcer notre cadre juridique en matière de cybersécurité, notamment dans le cadre de la transposition de la directive européenne NIS 2, qui fait l'objet du titre II du projet de loi. Il ne faut pas non plus oublier le titre I^{er}, consacré à la résilience des activités d'importance vitale et qui procède à la transposition de la directive sur la résilience des entités critiques (REC) ; et le

titre III, consacré à la résilience opérationnelle numérique du secteur financier qui procède à la transposition de la directive sur la résilience opérationnelle numérique du secteur financier (Dora).

Dans ce contexte, nous souhaitons vous entendre sur la manière dont vous percevez le projet de loi et les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du projet de loi par l'Assemblée nationale.

M. Philippe Luc, membre de Cyber Task Force et président d'Anozr Way. Je vous remercie pour cette invitation et pour l'attention que vous voudrez bien porter aux préoccupations que nous vous remontons. Je suis Philippe Luc, président d'Anozr Way, une société spécialisée en cybersécurité, membre du bureau national de l'Alliance pour la confiance numérique. Nous nous exprimons aujourd'hui en tant que témoins d'une évolution préoccupante de la menace cyber, des tactiques des attaquants et de l'adaptation parfois insuffisante des stratégies de défense. Malgré un niveau de maturité croissant des entreprises et de nos institutions, jamais elles n'ont été autant exposées.

Comment expliquer ce paradoxe ? Nous pensons que ceci est d'abord lié à une inadéquation entre nos stratégies de défense et celles des attaquants. Les défenses restent largement pensées selon des logiques techniques, alors que les attaques reposent sur une approche dynamique, opportuniste et surtout humaine. Le directeur général de l'Anssi a évoqué à juste titre la notion de menace systémique capable de fragiliser tout un système par simple effet domino.

Si nous avons progressé sur le terrain des vulnérabilités techniques, la principale faille aujourd'hui est humaine. Prenons un exemple concret : un salarié clique sur un lien d'hameçonnage, un logiciel malveillant s'introduit, se propage via des interconnexions à d'autres entreprises, et finalement, l'ensemble d'un réseau économique est menacé. Le point d'entrée est souvent humain, et cet hameçonnage n'est qu'un point de départ. Aujourd'hui, les vulnérabilités humaines sont devenues multiples et complexes. Un attaquant peut exploiter des informations personnelles, comme une dette de jeu en ligne, pour faire pression sur un salarié dont il pourrait même louer les identifiants, ou les avoir volés déjà au préalable.

Cela devient le modèle économique du cybercrime et le point commun de bon nombre d'attaques qualifiées de techniques. Le facteur humain est désormais le principal vecteur de propagation des menaces systémiques. Les attaques par ingénierie sociale, l'hameçonnage, les *deep fake* utilisent des données personnelles disponibles en source ouverte – on parle de renseignements d'origine source ouverte (Osint). Les attaquants maîtrisent parfaitement ces techniques pour manipuler les individus. Nos stratégies de défense sont inefficaces, car nos dispositifs classiques de sécurité ne prennent pas en compte la réalité du risque humain, et tous les audits de sécurité classique que l'on peut mener ne détectent pas les comportements à risque, les mots de passe réutilisés ou les informations sensibles, nécessaires à la réalisation de ces scénarios d'attaques par ingénierie sociale.

J'en profite également pour préciser qu'on ne résoudra pas le problème du facteur humain uniquement par des sessions de *e-learning* ou des tests d'hameçonnage. Nous devons passer d'une posture statique de sensibilisation à une posture active de gestion du risque humain par un *monitoring* continu du risque d'exposition de ces utilisateurs aux attaques par ingénierie sociale. Cela devra impérativement être intégré dans le référentiel d'application qui accompagnera ce projet de loi.

La France possède déjà un savoir-faire solide en la matière. Dans ce contexte, la directive NIS 2 représente une opportunité cruciale. Elle consacre l'intégration du facteur humain comme un élément central de la résilience cyber. Pourtant, dans sa première version, le projet de loi français ne faisait aucune mention des vulnérabilités humaines. Il a fallu un amendement du Sénat pour les réintroduire, soit une avancée majeure que nous saluons. Cependant, nous devons aller plus loin. Au-delà de l'établissement d'un cadre technique, la directive NIS 2 constitue un véritable changement de paradigme. Elle nous invite à penser la cybersécurité non plus uniquement en termes de protection, mais en termes de gestion active du risque, en intégrant pleinement les erreurs humaines.

Cela suppose impérativement de travailler sur les définitions. La définition de vulnérabilité a été intégrée, mais la notion de cyber menace ou d'approche « tous risques » reste toujours absente du corpus juridique. De leur côté, nos voisins allemands et italiens les ont intégrées, et l'Allemagne vise explicitement les considérants 78 et 79 de la directive, qui détaillent cette approche globale. Les Italiens en ont même tiré une définition à part entière. De fait, on ne peut pas atteindre un haut niveau de résilience convenable si l'on ne définit pas précisément les termes de risque, de menace et de vulnérabilité. Le sujet n'est pas uniquement français, mais se situe au niveau européen. Il est nécessaire que nous nous accordions sur une même définition en Europe.

En conclusion, si nous voulons sortir de cette spirale d'attaque, nous devons changer de regard. Le cyber criminel moderne n'a pas besoin de forcer la porte ; il sait que quelqu'un lui ouvrira ou qu'une clé traînera sous le paillasson. La directive NIS 2 nous offre l'opportunité d'abandonner une posture purement défensive pour construire une cybersécurité fondée sur l'anticipation, la pédagogie et la gestion proactive du risque humain.

Mme Garance Mathias, administratrice du Clusif. Les propos du Clusif se concentreront particulièrement sur le titre II relatif à la transposition de la directive NIS 2, un enjeu extrêmement important, y compris pour la collectivité du Clusif, peut-être la seule association à être reconnue d'utilité publique depuis la fin de l'année 2024. Dans le cadre de cette transposition de textes très ambitieux, il importe de ne pas se concentrer uniquement sur la France métropolitaine, mais d'appréhender la richesse de l'ensemble de nos territoires. Au sein de l'association que nous représentons aujourd'hui, nous avons également la chance de disposer de clubs de la sécurité de l'information en réseau (Clusir) outre-mer.

Ensuite, il nous semble très important de revenir plus spécifiquement sur le choix des référentiels. Je cède la parole à M. Dubois, qui abordera la question des sanctions, mais aussi la notification des incidents, un aspect opérationnel très important qui concerne l'ensemble des acteurs, collectivités, administrations ou entreprises. Votre projet de loi doit être envisagé comme une opportunité et non uniquement comme une contrainte.

M. Michel Dubois, administrateur du Clusif. Le Clusif appelle à établir un référentiel qui s'appuie sur la famille des normes ISO 27000, à l'instar de la Belgique. En effet, la norme ISO 27002 présente notamment l'avantage d'être opérationnelle dans toute l'Europe et de constituer un élément clé dans la mise en conformité des organisations. La norme ISO 27001 étant certifiante, une approche similaire à la Belgique proposant soit une certification 27001, soit une conformité à un référentiel local, semble constituer une approche intéressante.

M. Benjamin Leroux, administrateur du Clusif. Il est important que ce référentiel soit reconnu dans les autres pays de l'Union européenne. À ce titre, une norme comme ISO peut être intéressante. Si elle n'est pas finalement retenue, il faudra que le référentiel national puisse documenter sa compatibilité avec les autres référentiels locaux.

M. Michel Dubois. Un autre aspect concerne notamment la partie relative aux référents. Nous sommes favorables à une obligation pour les structures éligibles à NIS 2 de disposer d'un référent, que l'on pourrait appeler référent cyber sécurité, référent sécurité numérique ou tout simplement responsable sécurité des systèmes d'information (RSSI). Ce référent aura un lien direct avec la direction de l'organisme, comme son comité exécutif et disposera de la légitimité et du soutien nécessaires aux travaux de mise en conformité et d'entretien dans le temps de cette conformité. Ce référent sera également le point de contact référent de l'Anssi.

M. Benjamin Leroux. Pour le Clusif, les entités publiques doivent également pouvoir être sanctionnées en cas de manquement, comme les entreprises privées. Il s'agit de la condition *sine qua non* d'une bonne prise de conscience de la part de la sphère publique. Il faut malheureusement parfois en passer par là pour engager une prise de conscience et les travaux de mise en conformité. La responsabilité du dirigeant ne doit pas nécessairement se traduire par des sanctions pénales. La logique consiste à faire prendre conscience de la nécessité de lancer et d'entretenir des travaux de mise en conformité, pour la maîtrise du risque cyber.

Mme Garance Mathias. En matière de sanctions, l'opinion du Clusif se rapproche de l'avis donné il y a déjà quelques mois par le Conseil d'État, notamment sur le point 9 : « *il n'en va pas de même pour les collectivités territoriales et de leurs regroupements et d'établissements, en l'absence des dispositifs d'effet équivalent et qu'en conséquence, cette exemption ne peut être admise* ».

M. Michel Dubois. Un autre point concerne la notification des incidents. Nous appelons à la mise en place d'une plateforme unique et d'un formalisme

commun à toutes les entités pouvant être en attente de ces notifications, par exemple la Commission nationale de l'informatique et des libertés (Cnil), l'Anssi ou encore l'Autorité de contrôle prudentiel et de résolution (ACPR) en ce qui concerne le règlement Dora. Ce point est particulièrement structurant pour les entités assujetties à Dora et à NIS 2. Une telle plateforme nous semble être un facteur de simplification et d'accélération des procédures pour les référents.

M. Benjamin Leroux. Enfin, nous savons d'expérience que les organisations présentent des niveaux de maturité très variables par rapport à la problématique cyber. Nous suggérons de nous inspirer de ce qui a été réalisé en Belgique avec Safeonweb, qui propose une très belle plateforme documentée pour la compréhension des mesures et le suivi de leur mise en application.

M. Jean-Noël de Galzain, président d'Hexatrust. Je me concentrerai pour ma part sur un aspect qui me paraît important, dévoilé récemment par le rapport d'Asterès : aujourd'hui, 83 % des achats de produits et services numériques réalisés en Europe sont effectués auprès de fournisseurs extra-européens, particulièrement auprès des Gafam. Nous ne résoudrons pas notre problème de dépendance numérique en continuant avec le modèle actuel. La cybersécurité constitue un moyen clé de reprendre une part de contrôle sur notre vie numérique.

Un aspect clé de cette directive NIS 2 concerne l'accompagnement des utilisateurs. À ce titre, je rejoins les propos tenus précédemment concernant le *monitoring* continu des risques. Il s'agira de s'appuyer sur un certain nombre de dispositifs pour la plupart existants. Ils sont portés par une industrie émergente et bénéficient parfois d'une certification de la part de l'Anssi. Nous pensons qu'il faut insister dans tous les textes relatifs au numérique et à la cybersécurité sur la protection des données et l'usage de solutions certifiées, à chaque fois que cela est possible, pour aligner les recommandations de l'Anssi ou des organismes européens avec les travaux de la filière.

Nous estimons aussi que l'accompagnement doit se concentrer sur l'ensemble du tissu de PME sous-traitantes des grandes organisations, qui constituent aujourd'hui le « maillon faible », car elles manquent de moyens, de compétences et de ressources. Ces dernières sont directement affectées par cette réglementation et devront être accompagnées sur tous nos territoires. De nombreux travaux sont menés par la filière pour y parvenir.

La directive NIS 2 constitue une chance de mettre l'industrie de la cybersécurité et l'industrie du numérique au service des besoins des utilisateurs. Il s'agit d'une opportunité pour alimenter une politique industrielle résolument tournée vers les utilisateurs, autour d'un nouveau standard de la gestion du risque, de la gouvernance de la cybersécurité. Il faut capitaliser sur la directive NIS 2 pour aligner les utilisateurs et leurs besoins, l'État qui veille à la sécurité et à l'accès de tous à la sécurité, et l'industrie qui fabrique des solutions et propose des services pour répondre à ces besoins.

Deux comités stratégiques de filière, le comité stratégique de la filière industrie de sécurité et le comité stratégique de la filière logiciels et solutions numériques de confiance ont instauré des organes de travail permanents entre l'État, l'industrie et les utilisateurs. Ils doivent être utilisés au maximum pour traiter les problèmes concernant les interactions entre les utilisateurs et l'industrie et les aligner avec la volonté de standardisation et de normalisation de la directive NIS 2.

Je souhaite à ce titre mentionner une initiative qui s'est déroulée il y a trois ans, dans le cadre du dispositif France Relance, au service des hôpitaux et des collectivités locales, en portant l'effort sur la demande de ces utilisateurs, en les aidant et en les incitant à s'équiper. Cette initiative a démontré que nous étions en mesure de répondre aux besoins des utilisateurs en matière de cyber lorsque les différentes composantes travaillent de manière coordonnée. Grâce à l'investissement, notamment à travers le crédit d'impôt recherche (CIR) ou d'autres dispositifs d'aide à l'innovation, nous disposons aujourd'hui d'une industrie émergente extrêmement performante, qui pourra se mettre au service des utilisateurs à l'occasion de la mise en place et de la mise en œuvre de cette directive NIS 2.

De nombreux efforts ont été régulièrement produits pour aider à la sensibilisation. Aujourd'hui, l'intelligence artificielle (IA) doit être au maximum utilisée pour rendre l'audit plus accessible au plus grand nombre, de manière systématique. Nous avons nous-mêmes œuvré en réunissant les adhérents pour créer un « HexaDiag », qui permettra aux entreprises de toute taille et de tout niveau d'expertise cyber d'accéder à un premier niveau de diagnostic. Nous sommes allés plus loin dans le cadre de l'« HexaSearch », pour permettre à des organisations de trouver des solutions numériques européennes et souveraines alternatives à celles qui existent par ailleurs et sur lesquelles le contrôle est difficile à opérer.

Mme Bénédicte Pilliet, présidente de CyberCercle. Mon intervention a pour objet d'insister sur les points d'attention qui nous semblent majeurs. Pour CyberCercle, la transposition de ces trois textes européens dans notre droit représente une occasion unique de renforcer la cohérence, la lisibilité, la clarté et l'efficacité de la réglementation en matière de cybersécurité et des politiques publiques qui y sont associées.

À ce titre, j'aborderai six points qui nous semblent particulièrement importants pour renforcer au sein du projet de loi la cohérence entre les différents dispositifs prévus par les trois textes, mais aussi la cohérence avec les textes et dispositifs existants. Le premier point concerne la nécessité d'une stratégie nationale. L'article 5 *bis* introduit par le Sénat, qui pourrait d'ailleurs être remis en cause par le gouvernement au prétexte que des stratégies plus globales sont en cours de rédaction, nous semble indispensable.

L'élaboration d'une stratégie inscrite dans la loi permettra à l'ensemble des acteurs concernés d'avoir régulièrement un cap et un cadre de référence, mais aussi de mieux comprendre l'organisation et la coordination au sein de l'État et les responsabilités de chacun. Il s'agit ainsi de coordonner dans un même cadre et vers

les mêmes objectifs les actions de tous et d'assurer la cohérence des dispositifs. La nécessité d'une stratégie nationale claire de cybersécurité a d'ailleurs été évoquée à plusieurs reprises lors de vos auditions précédentes, notamment celle des collectivités. Cette stratégie permettra également au Parlement de contrôler et d'évaluer l'efficacité des mesures prises et de la dépense publique consacrée à la cybersécurité. Afin d'optimiser sa rédaction, il serait pertinent qu'une commission réunissant les parties prenantes élabore ses stratégies, comme c'est le cas pour le Livre blanc de la défense et de la sécurité nationale.

Le deuxième point concerne la cohérence dans les acteurs impliqués. Ainsi, l'absence des ministères est inexplicable dans la mise en œuvre de NIS 2. Au-delà de notre conviction que pour être efficace envers des secteurs d'activité par nature très différents les uns des autres, une approche par métier est capitale. Il s'agit là de mettre en cohérence les trois textes transposés quant au rôle des ministères coordonnateurs des secteurs d'activité concernés par les directives REC, NIS 2 et Dora. Les quelques centaines d'opérateurs d'importance vitale mentionnés au titre I^{er} du projet de loi sont identifiés et suivis par les ministères coordonnateurs du secteur d'activité auquel ils appartiennent.

Le même principe s'applique pour le titre III du projet de loi : les autorités financières, dont les ministères économiques et financiers, suivent et contrôlent les quelques milliers d'acteurs visés par le règlement Dora. Mais alors que dans le titre II, il s'agit de suivre des dizaines de milliers d'entités visées par la directive NIS 2, seule l'Anssi est en charge de l'ensemble dans le texte, les ministères étant finalement exclus de tout le processus Pourtant, ce sont bien les ministères qui, de fait, connaissent le mieux les métiers, les dépendances et les conséquences d'une défaillance d'un opérateur et les conditions de résilience dans les secteurs d'activité dont ils ont la charge. Ajoutons que dans un objectif d'optimisation de l'action des acteurs et des moyens de l'État, le rôle des ministères relève du bon sens.

Il nous semble donc essentiel d'introduire les ministères coordonnateurs dans le titre II du projet de loi, au moins dans les quatre étapes du processus : la validation et le complément éventuel des listes des entités essentielles et importantes (article 12) ; la définition des objectifs de sécurité et des référentiels d'exigence (articles 14 et 15) ; les contrôles (article 29) et la commission des sanctions (article 36).

Le troisième point est relatif à la cohérence dans les objectifs de sécurité et les référentiels de mesures techniques et organisationnelles. Dans l'article 14, un décret fixe les objectifs de sécurité auxquels doivent se conformer les entités essentielles et les entités importantes. Cependant, il n'est pas précisé qui définit les objectifs, ni comment. Pourtant, un peu plus loin dans le même article, ces éléments sont indiqués pour les référentiels d'exigence technique et organisationnelle.

Dans l'article 15, les entités qui mettent en œuvre tout autre référentiel reconnu équivalent par l'Anssi peuvent s'en prévaloir lors d'un contrôle. Il y a là une incohérence. Ces référentiels équivalents devraient également, comme dans

l'article 14, être définis par les métiers, d'autant plus si ces référentiels sont sectoriels, exigés par les marchés ou issus d'autres réglementations s'imposant à eux.

Enfin, dans son article 25 portant sur la normalisation, la directive NIS 2 précise « *qu'afin de favoriser la mise en œuvre convergente des mesures de gestion des risques en matière de cybersécurité, les États membres encouragent le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information* ». Cet article important de la directive NIS 2 n'a pas été transposé. Pour nous, il y a là une occasion manquée d'une harmonisation au niveau européen ou international, qui aurait soutenu la compétitivité de nos acteurs économiques. Au contraire, le renvoi de l'article 14 du projet de loi examiné par votre commission annonce un énième référentiel franco-français dont le coût de la conformité technique et organisationnelle s'ajoute à celui du coût de la conformité aux normes que les entreprises doivent respecter pour gagner des marchés. En outre, nous pointons les oppositions existantes entre les prescriptions du projet de référentiel Anssi et les obligations des actes d'exécution pris en application de Dora au niveau européen.

Le quatrième point concerne la cohérence et la clarté, voire l'égalité devant la loi en ce qui concerne les contrôles. L'article 29 précise que les contrôles de l'Anssi peuvent prendre plusieurs formes, dont celle d'audits réguliers et ciblés réalisés par un organisme indépendant désigné par l'Anssi. Le coût de cette forme de contrôle est à la charge des personnes contrôlées alors que, pour les autres formes, il relève de l'Anssi. Il nous semblerait pertinent d'encadrer le terme « réguliers » et de préciser à quoi correspond un organisme indépendant désigné par l'Anssi. Pourquoi existe-t-il une telle différence de traitement des entités ? Qui choisira parmi les différentes formes de contrôles celles qu'une entité devra subir et donc si ce contrôle sera ou non à sa charge ?

Le cinquième point est lié à la cohérence dans les sanctions. Deux points sujets à questionnement figurent dans l'article 37 relatif aux sanctions. La commission des sanctions peut prononcer une amende administrative pour les entités essentielles et importantes, à l'exception des administrations et des collectivités territoriales. L'amende ne concerne donc que les entreprises privées. Pourquoi l'interdiction d'exercer des responsabilités pour les dirigeants des entités essentielles ne s'appliquerait-elle pas à l'administration ? De plus, comment appliquer cette interdiction à l'élu d'une collectivité ? Pour plus de transparence et pour éviter d'avoir le sentiment qu'aucune sanction ne sera prononcée contre l'administration, cet article pourrait ainsi préciser les moyens utilisables par l'État, en lien avec l'avis du Conseil d'État du 6 juin 2024.

Enfin, le dernier point sur lequel nous nous permettons d'insister porte sur l'exploitation de l'information relative à la menace, non seulement par les entités visées par NIS 2, mais également par leurs prestataires. Nous n'entrons pas dans le cœur des débats sur le sujet, qui agitent l'écosystème, mais constatons simplement que l'article 45 du règlement Dora donne un cadre à l'échange d'informations entre

les acteurs visés par Dora. Ne pas transposer l'article 29 prévu dans la directive NIS 2, portant sur le même sujet, introduit de fait une inégalité et une incohérence pour les entités soumises à Dora et à NIS 2.

Pour conclure, je voudrais citer le rapport d'activité 2024 de l'Anssi relatif au parcours de cybersécurité dans le cadre du programme de France Relance. Même si ce rapport partiel ne permet pas d'évaluer réellement l'efficacité des 100 millions d'euros dépensés pour les 945 entités publiques sélectionnées parmi plus de 1 600 candidatures, il met en évidence deux faits. Initialement, la note cyber moyenne des bénéficiaires de ce programme était de D+ soit une mauvaise note. Ainsi, treize ans d'empilement de réglementations s'imposant à la plupart de ces entités n'ont pas permis d'élever leur niveau de cybersécurité. Sans réglementation supplémentaire, le niveau de cybersécurité de ces entités est passé de D+ à B, c'est-à-dire de « mauvais » à « bon », grâce à ce programme, pour un montant équivalent voire inférieur à celui annoncé pour NIS 2.

Lors d'une audition de votre commission, les collectivités ont insisté sur la nécessité d'être accompagnées pour ne pas subir de nouvelles réglementations qui, seules, n'apportent pas de maturité. Il en est de même d'ailleurs pour les entreprises. Aussi, si nous comprenons le choix de la France d'inscrire les collectivités dans le cadre de cette loi, devant la croissance de la menace, nous nous interrogeons sur le choix de soumettre autant de collectivités à NIS 2, d'autant plus qu'aucune analyse de l'impact financier n'a été menée.

En conclusion, cette transposition constitue une opportunité de renforcer la cybersécurité de notre pays et sa résilience en élevant le niveau de maturité des acteurs et en les embarquant dans une dynamique vertueuse. Les questions concernent le niveau du curseur et l'accompagnement des acteurs par des politiques publiques adaptées dans un contexte budgétaire restreint. Le Sénat a permis d'améliorer substantiellement le texte initial du gouvernement en introduisant encore plus de cohérence entre les différentes parties du texte. Votre commission spéciale pourrait faire émerger un texte encore plus pragmatique.

M. Daniel Le Coguic, président de l'Alliance pour la confiance numérique. L'Alliance pour la confiance du numérique représente l'industrie française dans le domaine de l'identité numérique, de la cybersécurité, de l'intelligence artificielle et des infrastructures de confiance. Elle a naturellement contribué depuis un an aux différents groupes de travail. Je souhaite d'ailleurs remercier l'Anssi et son directeur général Vincent Strubel d'avoir organisé cette discussion structurée pour préparer la constitution de ce texte.

Nous avons, à de nombreuses reprises, présenté un certain nombre de propositions, notamment d'ajustement. Certaines ont été prises en compte lors de notre audition au Sénat. Nous vivons une période très particulière sur les plans géopolitique, économique, social et de la sécurité, où il est souhaitable de mettre en avant les intérêts de l'industrie française. Les parties prenantes que nous avons consultées nous ont toutes fait part de la nécessité de simplification et de lisibilité :

la directive ne doit être ni surtransposée, ni sous-transposée. Les cibles de NIS 2 sont aujourd'hui des entités peu matures dans le domaine de la cybersécurité. Elles doivent pouvoir comprendre le texte auquel elles sont soumises.

Ensuite, la divulgation de vulnérabilités nous semble être un point clé pour accroître la capacité de l'ensemble de ces entités à se défendre. Nous avons également proposé une incitation en direction des PME, un crédit d'impôt à définir, pour financer les investissements.

L'ACN soutient l'objectif général des trois textes, qui concerne l'augmentation de la résilience de la nation. Nous sommes attendus par nos citoyens. Mais il faudra être attentif à la mise en œuvre du texte. Nous soutenons les nombreux dispositifs d'ajustement qui ont été proposés, dans un objectif de simplicité et d'efficacité. Sur un horizon de trois ans, nous devrions atteindre l'objectif des 12 000 à 16 000 cibles à traiter.

Ce programme stratégique offre une opportunité pour l'industrie française de reprendre une place particulière, alors que nous vivons aujourd'hui un puissant déséquilibre entre l'industrie extra-européenne et l'industrie européenne dans le domaine de la cybersécurité. Si nous n'y prenons pas garde, la mise en œuvre du programme profitera à l'industrie extra-européenne qui possède déjà une part de marché de 80 %.

Il convient donc d'être très attentif aux conditions de mise en œuvre de ce programme. Nous proposons un objectif de transformation des investissements qui seront réalisés autour de NIS 2 et de Dora. Il s'agit ainsi de mettre en place un dispositif de mesures de l'empreinte de l'industrie française en particulier, qui sera la conséquence des investissements des établissements financiers, des institutions de santé, des collectivités locales et des entreprises.

En résumé, nous souhaiterions que le texte mentionne un objectif de 80 % de transformation et la mise en place d'un dispositif de mesure de l'augmentation de cette empreinte dans l'équipement de toutes les cibles. Cela compléterait les dispositifs de France 2030 sur l'innovation. Il s'agit bien de mettre en cohérence les programmes NIS 2 et Dora avec les objectifs économiques de l'industrie française.

En conclusion, il faut faire simple, il faut aller vite, il faut collaborer tous ensemble, qu'il s'agisse des associations d'utilisateurs, mais aussi des associations d'entreprises. Nous formons le vœu que se poursuive cette discussion structurée entre l'industrie et les pouvoirs publics, pour une mise en œuvre efficace au service des citoyens, des entreprises, des organisations publiques, de la cybersécurité et de la sûreté de notre nation.

M. Arnaud Martin, vice-président du Cesin, directeur des risques opérationnels de la Caisse des dépôts. Nous représentons le Cesin, le club des experts de la sécurité de l'information et du numérique, une association loi 1901 créée en 2012 dans un objectif de professionnalisation et de promotion de la cybersécurité. Ce lieu d'échange, de partage de connaissances et d'expériences

permet ainsi la collaboration et la coopération entre pairs, mais également entre ses experts et les pouvoirs publics.

Il participe à des démarches nationales et il est force de proposition sur des textes réglementaires, guides et autres référentiels. Le Cesin compte parmi ses membres plusieurs organismes et institutions, ainsi que 1 200 membres qui sont issus de tous secteurs d'activité : industries, ministères et entreprises, dont la plupart des grands acteurs du CAC 40 et du SBF 120. Mylène Jarossay et moi-même en sommes vice-présidents. Mme Jarossay est directrice de la cybersécurité du groupe LVMH et je suis directeur des risques opérationnels du groupe Caisse des dépôts. À ce titre, nous sommes assujettis à NIS 2 d'un côté et à Dora de l'autre.

Nos retours d'expérience dans le cadre de cette audition sont bien évidemment ceux de notre propre expérience, mais également la consignation de l'ensemble des travaux qui ont été menés. Nous souhaitons tout d'abord souligner l'avancée notable que constitue l'ajout de deux articles au niveau du titre II, le 5 *bis* et le 16 *bis*. L'article 5 *bis* réaffirme que la déclinaison des textes de cybersécurité et de résilience se fait désormais dans un cadre faîtier, porté par la stratégie nationale en matière de cybersécurité de la France.

Si ce texte est la déclinaison de la stratégie qui a été travaillée au niveau du secrétariat général de la défense et de la sécurité nationale (SGDSN), nous insistons sur une des recommandations essentielles : la simplification globale du millefeuille réglementaire, à laquelle votre projet de loi participe bien évidemment. Le deuxième point concerne la réaffirmation du principe de non-affaiblissement des algorithmes de chiffrement dans votre texte dédié à la cybersécurité et à la résilience.

Mme Mylène Jarossay, vice-présidente du Cesin, directrice cybersécurité du groupe LVMH. Parmi les sujets propres au texte, je tiens à évoquer un certain nombre de points, en commençant par le lien entre Dora et NIS 2. Actuellement, les organismes assujettis à Dora sont évidemment focalisés sur leur mise en conformité par rapport à ce texte et s'interrogent. Il existe en effet une zone de flou dans leur éventuel assujettissement complémentaire à NIS 2, notamment les rôles et responsabilités que pourraient avoir la Banque centrale européenne (BCE) et l'ACPR vis-à-vis de l'Anssi.

Concernant NIS 2, une interrogation pèse sur les entreprises qui opèrent dans plusieurs pays européens et pour lesquelles le choix du référentiel par le groupe constitue un véritable casse-tête. Dans certains pays, les référentiels insistent plutôt sur l'analyse de risque, dans d'autres sur l'administration des systèmes d'information. Un groupe européen ou international ne s'y retrouve pas ; il est confronté à une complexification et non à une simplification.

La complexité concerne également l'éligibilité, c'est-à-dire le fait de savoir si l'on est assujetti ou non au texte. Il nous semble urgent que la France puisse très vite répondre aux entreprises concernant leur éventuelle éligibilité. Or un grand flou règne aujourd'hui. Les outils actuellement en place ne permettent pas aux

entreprises de le déterminer. En conséquence, elles sont en retard, parce qu'elles n'engagent pas réellement leurs démarches.

Ensuite, nous rejoignons les propos qui ont été tenus précédemment sur le sujet de la notification des incidents. Il est important de se demander pourquoi le texte cherche impérativement à établir des délais courts de notification des incidents. Dans la réalité, quantité de signaux arrivent tous les jours dans les entreprises. Il est très difficile de savoir sous vingt-quatre heures si un signal est un « faux positif » ou s'il constituera le début d'une catastrophe. Il est donc très compliqué de produire une notification dans un tel délai, particulièrement s'il n'existe pas de guichet unique, d'autant plus pour une société paneuropéenne, qui devrait reproduire cette notification dans tous les pays dans lesquels elle est implantée. À ce stade, l'effort d'une entreprise ne doit pas être concentré sur la notification, mais sur la mise en place de renforts et la communication avec ses prestataires, d'autant plus qu'un incident sur deux provient de la chaîne d'approvisionnement.

Si finalement une attaque n'en est pas une ou qu'elle a été contenue très vite, donnons-nous la possibilité d'annuler une déclaration d'incident, et de ne pas faire courir le risque que cette déclaration porte éventuellement tort à l'entreprise. Cela nous paraît très important, afin que la notification des incidents demeure vertueuse et serve réellement à protéger.

Un autre point de vigilance concerne la déclinaison des exigences vis-à-vis des sous-traitants, des prestataires. Les entreprises éprouvent des difficultés pour mettre en place ces exigences. Aujourd'hui, il est question de mener des audits sur les fournisseurs, mais rappelons qu'en matière de cybersécurité, un audit ponctuel a peu de valeur : en réalité, la sécurité évolue tous les jours. Il faut peut-être revoir la façon dont on mesure finalement la capacité des tiers à se conformer au texte et le poids contractuel associé. De fait, une réflexion doit être conduite dans ce domaine, dans la mesure où le levier contractuel est très long et très difficile à mettre en place. De plus, la notion d'audit, très coûteuse n'est pas forcément adaptée au monde cyber.

Le dernier point est relatif au référent cyber, qui est naturellement essentiel, dans la mesure où le risque cyber figure parmi les trois principaux risques des entreprises. Quel que soit le nom qui sera choisi, je préférerais que le terme de RSSI soit abandonné, dans la mesure où le dirigeant de l'entreprise est, *in fine*, le responsable.

M. Éric Bothorel, rapporteur général. Cette transposition de la directive européenne était attendue et même espérée par votre écosystème. Elle conforte les actions que vous avez commencées de façon volontaire il y a plusieurs années, pour nombre d'entre vous. Elle confirme que les craintes que vous exprimiez sont bien réelles. Lors des auditions du Sénat, vous avez rappelé l'évolution majeure de ce texte, qui passe d'une logique des seules infrastructures à celle des organisations et donc des personnes.

Il peut être considéré qu'à ce stade, le projet de loi ne fait pas de place à l'humain. Je souhaite donc vous interroger sur les évolutions – législatives ou autres – afin que les différentes personnes, les salariés, les fonctionnaires et les élus soient mieux associés au projet collectif de résilience.

Lors des dernières auditions, plusieurs acteurs nous invitaient à inscrire dans la loi un certain nombre de définitions, et vous l'avez aussi rappelé ce matin. Ce n'est pas forcément l'usage français, alors que l'Europe procède beaucoup par définition et normalisation. Pourriez-vous nous indiquer quels sont les termes qui nécessiteraient d'être inclus dans la loi ?

Par ailleurs, nombre d'acteurs soulignent tout à la fois l'excellente qualité du travail préparatoire et du dialogue avec l'Anssi. Mais les mêmes acteurs commencent à nous faire part de leurs interrogations sur le trop grand nombre de renvois à des décrets. Ils semblent préférer que les députés soient plus précis dans leur rédaction, allant parfois jusqu'aux détails. Partagez-vous ce point de vue ? Comment envisageriez-vous cette intégration dans la loi, par exemple du référentiel, compte tenu du nombre de détails que vous voulez voir inscrits ? Enfin, j'aimerais que nous parlions de l'Osint, du volet assurantiel.

Mme Anne Le Hénanff, rapporteure. La plupart d'entre vous travaillent sur la sensibilisation et l'accompagnement depuis des années. Mais ces actions de sensibilisation n'engendrent pas forcément une amélioration du niveau de cybersécurité des entités, particulièrement les collectivités locales. Or la directive entraînera un impact élargi sur l'ensemble des territoires. Comment pouvons-nous sensibiliser plus rapidement les collectivités locales ?

Comment comptez-vous sensibiliser et accompagner ce changement, dans le cadre de NIS 2 et au-delà, auprès des prestataires, des sous-traitants et des clients, qui ne sont pas directement dans les 15 000 entités mentionnées, mais qui devront sans doute procéder à des mises à jour ? Comment allez-vous prendre votre part à la cyber-résilience ?

Estimez-vous que la labellisation des entités est pertinente ? Est-il utile pour une entreprise d'indiquer à des clients, des prestataires, des sous-traitants qu'elle est en conformité ou en cours de conformité avec NIS 2 ? À ce sujet, il est souvent question de proportionnalité, mais peut-on également parler de proportionnalité sur la mise en conformité ?

Madame Mathias, vous avez mentionné la nécessité de tenir compte spécifiquement des territoires d'outre-mer. Faut-il en conclure que vous estimez que la rédaction actuelle est insuffisante à ce titre ? Avez-vous en tête des mesures spécifiques ?

Enfin, je souhaiterais connaître l'avis de chacun sur la notification d'incident. Constitue-t-elle le mode d'emploi adapté en termes de mécanismes, de principes et de mesures ?

M. Daniel Le Coguic. Ma réponse se concentrera sur la sensibilisation et l'information pour préparer l'accompagnement. Nous avons identifié deux cibles dont la maturité est insuffisante : les PME et certaines collectivités locales, vers lesquelles des efforts de communication doivent être réalisés. De son côté, l'industrie doit aussi fournir un travail pour mettre en place des solutions très lisibles et compréhensibles pour les cibles.

Si la mise en œuvre de Dora est plus concentrée sur la région parisienne, NIS 2 concernera l'ensemble du territoire français, ce qui nécessitera d'impliquer tous les acteurs. À ce titre, les campus cyber devraient être intégrés dans le dispositif. Les régions seront également intéressées, en raison de leurs compétences en matière de politique économique. Le « retour sur investissement » de NIS 2 doit ainsi concerner les territoires. En résumé, en compagnie de l'Anssi, nous devons travailler à une collaboration globale de tous les acteurs nationaux et régionaux en faveur du programme de sensibilisation et de communication, et ensuite de mesure de la politique industrielle.

M. Yoann Kassianides, délégué général de l'Alliance pour la confiance numérique. L'Osint constitue un enjeu majeur. Les attaquants se servent d'outils essentiellement fondés sur les vulnérabilités humaines. Dans ce cadre, l'Osint représente une réponse efficace et sa pratique est aujourd'hui extrêmement répandue. Néanmoins, l'ensemble des acteurs de ce domaine s'interrogent sur le cadre juridique applicable.

L'ACN mène depuis maintenant deux ans des travaux, en partenariat avec la chaire Cyber de l'Institut des hautes études de défense nationale (IHEDN) rassemblant de nombreux acteurs de la sphère étatique (pouvoirs judiciaires, services du ministère de l'intérieur), la Cnil, des entreprises, des avocats. Le constat est extrêmement clair : le droit actuel ne permet pas aujourd'hui d'appréhender correctement cette pratique de l'Osint.

En conséquence, il est extrêmement difficile de construire des modèles économiques, faute de clarification des zones d'ombre entre ce qui est autorisé et ce qui ne l'est pas. Nous proposons donc de créer un droit commun de l'Osint. À l'heure actuelle, le droit applicable est très morcelé et limité à certains domaines restreints, par exemple le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) ou l'administration fiscale.

Ce cadre préciserait notamment que la pratique de l'Osint est libre tout en étant contrebalancée par l'ensemble des libertés individuelles et publiques et par la protection des secrets. Il permettrait de donner des possibilités d'exercer l'Osint pour des motifs légitimes. L'objectif consiste à définir clairement dans quelles circonstances cette pratique est permise et de distinguer les cas où elle ne l'est pas. Ce cadre juridique aurait également pour but de modifier certains articles du code pénal, afin de simplifier leur interprétation et d'éviter des situations aberrantes.

La situation actuelle, marquée par une divergence entre l'esprit de la loi et sa lettre, conduit à des résultats contre-productifs. Quelques mesures extrêmement simples sur la création d'un droit commun de l'Osint permettraient de remédier à ces problèmes de manière assez claire. Par conséquent, nous souhaitons porter ce sujet au débat.

M. le président Philippe Latombe. Les collectivités nous ont parlé de la fin programmée des financements des centres d'alerte et de réaction aux attaques informatiques (CSIRT). Cet outil vous est-il utile ? Faudrait-il les pérenniser sous une forme ou sous une autre en termes de financement ou de statut ?

Ensuite, comment pourrions-nous modifier le statut des divulgations des vulnérabilités *zero-day* afin de résoudre les problèmes juridiques qu'elles posent aux acteurs qui les identifient et souhaitent en parler à la communauté pour accélérer les correctifs ? Avez-vous des avis sur ce sujet ?

Mme Dorothée Decrop, déléguée générale d'Hexatrust. Je me concentrerai sur l'aspect humain et l'accompagnement des acteurs concernés par les entités importantes, ainsi que sur la chaîne de sous-traitance. Nous collaborons avec la direction générale du travail (DGT) pour intégrer le risque cyber dans le document unique d'évaluation des risques et de prévention (Duerp), afin de sensibiliser les entreprises, à droit et coût constants. Il est crucial d'intégrer ces risques dans la gestion courante, en utilisant des outils existants pour sensibiliser les entreprises de manière homogène au niveau territorial.

L'accompagnement des entreprises est essentiel. Nombre d'entre elles ignorent si elles deviennent des entités importantes selon l'article 12. Un travail sur les codes NAF (nomenclature d'activités française) et NACE (nomenclature d'activités européennes) permettrait de clarifier la situation, offrant une meilleure lisibilité et l'identification rapide des entreprises concernées. Cela garantirait, sous la forme NACE, une interprétation uniforme des entités importantes au niveau européen et permettrait d'homogénéiser les entreprises qui seront cibles ou se saisiront de cette opportunité. Chez Hexatrust, nous sensibilisons les fédérations professionnelles soumises à NIS 2 par un module de sensibilisation de premier niveau. Nous établissons des partenariats pour utiliser l'« HexaDiag », notre démarche de cybersolidarité permettant un autodiagnostic rapide et autonome et des résultats immédiats. Dans un deuxième temps, les entreprises contactent des professionnels pour réaliser des démarches bien plus complètes.

Nous sommes membres du Campus cyber national, nous programmons des interventions et actions communes avec les campus régionaux, et nous sommes partenaires de l'association CoTer. Nous irons également sensibiliser les collectivités territoriales à ces enjeux, au même titre que d'autres associations.

Concernant la labellisation NIS 2, nous manquons encore de documentation précise. La cybersécurité doit rester agile et adaptable, accessible juridiquement,

avec des directives claires et dynamiques pour éviter de créer des barrières à l'entrée pour certains professionnels. En résumé, il est difficile de se prononcer à ce stade.

M. Jean-Noël de Galzain. Concernant l'assurance, je pense que la cybersécurité devrait être considérée comme un risque, au même titre que d'autres types de risques. Elle devrait donc faire partie intégrante de l'obligation d'assurance en responsabilité civile des entreprises. Une entreprise qui respecte des normes telles que celles de Dora ou NIS 2 pourrait ainsi obtenir un accès facilité à l'assurance et une couverture en cas d'incident. En effet, comme l'a mentionné le directeur de l'Anssi, les attaques coûtent cher, nécessitent une réaction rapide et des compétences spécialisées pour rétablir la situation rapidement. L'assurance peut donc aider à gérer concrètement les problèmes lorsqu'ils surviennent.

M. Michel Dubois. Le constat est unanime depuis plusieurs années : la sensibilisation ne fonctionne pas ; c'est un échec. Il manque un chef de file. Dans ces conditions, il serait pertinent de mettre en avant cybermalveillance.gouv.fr, qui traite ce sujet. Ensuite, il faut un référentiel des démarches et des supports. L'Anssi a mis en place un « cyber dico » régulièrement mis à jour. Il serait utile de mettre en lumière cet outil pour disposer d'un référentiel unique des définitions en cybersécurité. Des labels ont été établis par l'Anssi pour les formations avec SecNumedu.

Il serait donc intéressant de valoriser ces labellisations dans la loi. Enfin, cybermalveillance.gouv.fr a développé plusieurs fiches thématiques de sensibilisation accessibles à tous. Le module de formation en ligne (Mooc) de l'Anssi constitue également un support disponible.

En réalité, il manque une obligation légale de sensibilisation et de formation. Il pourrait exister une disposition similaire à celle de la sécurité incendie, où l'employeur doit former ses employés au moins une fois par an. La notion du référent en cybersécurité dans l'entreprise pourrait porter cette responsabilité.

Enfin, un maillage local fondé sur les Campus cyber peut être officialisé. Par exemple, le Clusif dispose de représentations régionales en France qui peuvent relayer ces messages, garantissant ainsi un continuum entre un référentiel, un chef de file et des obligations légales.

M. Sébastien Garnault, fondateur de CyberTaskForce. Comment transmettre le message aux collectivités ? Je propose d'utiliser le salon des maires, moment important pour les collectivités, pour communiquer avec les communes. Cependant, elles expriment souvent des besoins financiers. Il faudrait donc accompagner davantage les petites collectivités et réallouer les budgets en conséquence.

Ensuite, les questions soulevées par Bénédicte Pilliet sont pertinentes et méritent des réponses précises. Concernant l'assurance, l'article 5 de la Lopmi avait initié une démarche, mais le problème porte surtout sur le modèle économique.

Toutefois, il semble qu'il faille explorer comment des acteurs comme Stoïk réussissent à offrir une assurance cyber à l'échelle française et européenne.

Mme Anne-Elise Jolicard, responsable des affaires publiques d'Anozr Way. La loi de transposition était attendue, notamment en ce qui concerne l'appréhension des vulnérabilités. Nous saluons l'amendement du Sénat incluant le facteur humain parmi les vulnérabilités. Cependant, il est nécessaire d'aller plus loin pour atteindre les objectifs de la directive, en veillant à ce que les termes soient clairs et définis, en suivant l'exemple de nos voisins italiens, belges et allemands, qui ont défini l'approche « tous risques » à partir des considérants 78 et 79.

De fait, le besoin de pédagogie est patent. Il est communément admis que la faille essentielle est la faille humaine. Pour autant, les textes français n'insistent pas assez sur la menace induite sur les entreprises et l'ensemble des citoyens. La définition de ces termes est cruciale pour guider et expliquer le cadre de la cybersécurité. Cette clarification est nécessaire pour mieux appréhender les menaces dans le contexte français.

Le risque de surtransposition a été écarté par le Conseil d'État qui invite au contraire à définir les termes clés de la directive. L'article 14 pourrait ainsi mentionner la notion d'approche « tous risques » et viser expressément les considérants 78 et 79. Enfin, la notion de cybermenace a aussi été définie par nos voisins. Elle figure dans la directive et pourrait être ajoutée au titre de l'article 6.

M. Philippe Luc. Concernant l'introduction d'une formation obligatoire, il est essentiel de noter que la cybersécurité intéresse principalement les professionnels. Les utilisateurs se concentrent sur l'utilisation des outils numériques sans se préoccuper de leur sécurité, de la même manière qu'ils utilisent leur voiture, sans se soucier du fonctionnement de leur airbag. Il est crucial de fournir des connaissances de base et des bonnes pratiques, surtout pour les jeunes. Pour les adultes, une approche plus légère pourrait éviter de les détourner du sujet. Les efforts actuels de cybermalveillance.gouv.fr sont louables et il faudrait proposer davantage d'outils de protection. Nos salariés sont souvent plus sensibles à se protéger personnellement dans leur vie privée qu'à protéger leur propre entité. En conséquence, ce sujet devrait être travaillé en compagnie de cybermalveillance.gouv.fr.

S'agissant des CSIRT, je ne dispose pas des qualifications pour discuter du sujet du financement. En revanche, il est important de disposer d'un maillage local pour établir des relations de confiance avec les PME. Les structures locales comme les CSIRT jouent un rôle clé en sensibilisant et en répondant aux questions des entreprises, compensant ainsi le manque d'intérêt des acteurs locaux pour les grandes institutions de cybersécurité.

Mme Garance Mathias. La sensibilisation est un aspect extrêmement important, évoqué notamment dans les propositions formulées en octobre 2024 par la commission supérieure du numérique et des postes, notamment les

recommandations n° 1 et n° 2. Il s'agit ici d'inclure le grand public, c'est-à-dire tous les acteurs. Par exemple, en matière de sécurité incendie, ces pratiques sont devenues des réflexes bien ancrés alors qu'auparavant, elles n'étaient pas aussi bien prises en compte. Il est donc impératif que cela devienne, dès le début, un automatisme et que toute la population soit sensibilisée via des campagnes d'information. Je tiens également à saluer le travail effectué par cybermalveillance.gouv.fr, le 17Cyber, ainsi que les formations de l'Anssi, qui bénéficient au plus grand nombre. Au sein du Clusif, nos adhérents et salariés formés peuvent offrir des exemples pratiques qui permettent d'ancrer ces solutions grâce à des communications bénéfiques et des retours d'expérience constructifs relatifs au niveau de maturité.

Concernant les territoires d'outre-mer, il est crucial de prendre en compte leur niveau de maturité et leurs besoins spécifiques en rapport avec leur position géographique. Une approche adaptée selon les statuts de chaque territoire et assemblée territoriale, par exemple de Polynésie française, de Wallis-et-Futuna et de Saint-Pierre-et-Miquelon, est essentielle pour utiliser pleinement leur potentiel concernant la résilience opérationnelle.

Fort heureusement, nous avons parmi nos plus de 1 300 adhérents des utilisateurs et des offreurs résidant dans ces territoires. Leur contribution permet de renforcer ce dialogue. La loi, générale et absolue, peut constituer une aide pour impulser ce mouvement déjà initié par cybermalveillance.gouv.fr, l'Anssi et d'autres autorités. Enfin, des définitions claires permettraient une compréhension précise, nécessaire pour se positionner judicieusement.

M. Arnaud Martin. Pour compléter certains propos, je souhaite revenir sur le délai pressenti de trois ans. Dans le cadre de Dora, toutes les banques et assurances sont conformes depuis le 17 janvier 2025. Deux aspects nécessitent du temps : d'une part, les audits et tests, y compris ceux avec des tiers, et, d'autre part, la gestion des clauses contractuelles, dont l'absorption totale par les partenaires pourrait prendre environ trois ans. À titre d'exemple, le régulateur nous a bien indiqué que les premiers tests de pénétration fondés sur la menace (TLTP) ne seront pas diligentés en 2025, mais plutôt début 2026-2027.

Concernant la déclaration des incidents, il est essentiel que les entreprises se fondent sur des critères factuels pour déterminer leur obligation de déclaration. Ces aspects sont plus structurés sur la partie financière, en termes de nombre de critères impactants. Le principe de proportionnalité est également essentiel. La première déclaration sous quatre heures, qui se substitue d'ailleurs à la directive sur les services de paiement (DSP2), n'oblige qu'à transmettre les informations disponibles à ce moment-là, avant de les enrichir au fur et à mesure.

En matière assurantielle, les rapports annuels de l'Association pour le management des risques et des assurances de l'entreprise (Amrae) montrent une stabilisation par comparaison avec les années 2020-2021. Les assureurs sont désormais prêts à assurer et les conditions de souscription d'assurance se sont

améliorées. Cela incite à ne pas réguler un marché en cours de stabilisation sur le haut du marché, augmentant l'appétence des assureurs pour se positionner sur des segments moins matures.

À l'heure actuelle, aucun actuaire ne dispose d'un modèle prédéfini pour évaluer précisément la pérennité de ce marché. Cela ressort d'ailleurs du dernier rapport de l'Amrae, dont la publication est imminente. Cependant, nous observons que ce marché suscite un certain intérêt. En résumé, une régulation excessive dans un domaine en cours d'autorégulation ne constitue sans doute pas la meilleure approche, actuellement.

Enfin, concernant l'acculturation au risque lié à l'impact d'une interruption d'activité, il est crucial que tous les collaborateurs soient sensibilisés, mais une attention particulière doit être portée à la formation des conseils d'administration et des comités exécutifs, conformément aux directives de Dora.

Mme Mylène Jarossay. Monsieur Martin vient de mentionner l'importance pour les dirigeants d'être informés annuellement de l'évolution des menaces cybernétiques. Cette mise à jour n'apparaît pas comme une exigence excessive.

Le facteur humain reste un défi majeur, car malgré les efforts de sensibilisation, l'erreur humaine demeure une vulnérabilité. Le défenseur doit maintenir mille portes fermées, quand il suffit à l'attaquant d'en trouver une seule ouverte. En outre, les scénarios d'ingénierie sociale sont assez redoutables ; ils sont en outre augmentés par de l'IA. Il est essentiel de mettre en place des processus et des solutions techniques pour minimiser les risques engendrés par les erreurs humaines, notamment en distinguant les responsabilités des utilisateurs et des administrateurs des systèmes d'information. L'Anssi souligne le volet administration dans son référentiel de mesures, ce qui est judicieux. Il faut concentrer l'attention sur les informaticiens et trouver des subterfuges techniques de process, pour empêcher qu'un seul humain ne mette à terre une entreprise.

M. Daniel Le Coguic. Concernant la réglementation, il est important de distinguer ce qui relève du décret ou de la loi. Par exemple, le dernier décret pour l'application la loi de programmation militaire (LPM) de 2013 a été publié en 2024, soit onze ans plus tard.

Ensuite, dans une première version du projet de gouvernement, les missions de l'Anssi étaient précisées. Aujourd'hui, elles sont renvoyées à un décret en Conseil d'État. Il est crucial de définir clairement les missions de l'Anssi dans les textes législatifs, plutôt que de laisser certains aspects à des décrets en Conseil d'État. Il serait bénéfique également de privilégier dans le texte l'accompagnement plutôt que le contrôle strict. Enfin, la question des audits réguliers par des organismes indépendants pourrait être précisée dans la loi.

En conclusion, s'il revient au législateur de définir ce qui relève de la loi et ce qui peut être renvoyé à un règlement, il faudra éviter un certain nombre de pièges.

Mme Bénédicte Pilliet. En matière de sensibilisation, de nombreuses ressources sont produites par l'État, par cybermalveillance.gouv.fr. En revanche, elles demeurent méconnues de nombreuses collectivités. Il existe donc un enjeu d'amélioration de la lisibilité et de l'accessibilité des ressources produites par les différentes administrations auprès des acteurs, afin qu'ils puissent se les approprier.

Mais plus que sensibiliser, il nous faut convaincre les élus et les chefs d'entreprise que la cybersécurité n'est pas qu'un sujet technique, à part. Aujourd'hui, le numérique est présent dans l'ensemble de nos métiers, il est le facteur de développement majeur de nos organisations, il est utilisé pour créer de nouveaux usages au service des citoyens par les collectivités. Dès lors, la cybersécurité doit être envisagée comme un facteur de confiance, de pérennité des projets développés, d'attractivité, de développement ; mais aussi un facteur politique pour les élus. Pour s'en convaincre il n'y a qu'à observer les conséquences d'une cyberattaque réussie sur une collectivité, qui peut l'empêcher de conduire ses missions.

La sécurité du numérique constitue bien un sujet de gouvernance, d'organisation, de formation, de sensibilisation, de droit et de conformité. Mais avant tout, il s'agit d'un sujet de développement pour les entreprises et pour les collectivités. Afin de faire réfléchir les acteurs aux conséquences d'une attaque cyber sur leur organisation, nous avons organisé à Lyon un exercice de gestion de crise d'origine cyber, mais sans spécialistes cyber. À travers cet exercice, les élus ont pris conscience que ce sujet qu'ils voyaient réservé aux spécialistes était en réalité au cœur de la continuité de leurs missions.

À ce propos, le salon des maires offre effectivement une opportunité pour l'acculturation, mais le travail au quotidien est essentiel. Nous le menons sur les territoires, avec les associations des maires. L'enjeu consiste bien à enclencher une dynamique, à trouver un « sponsor », quelqu'un qui soit convaincu. C'est un travail de longue haleine, de proximité, continu, parfois un peu décourageant, mais toujours nécessaire.

M. Éric Bothorel, rapporteur général. Pourriez-vous revenir sur la simplification qui pourrait être apportée à une notification d'incident ? Vous avez formulé un certain nombre de propositions, mais pourrait-on envisager une plateforme commune dans laquelle vous retrouveriez, un plus petit dénominateur commun ?

Ensuite, j'ai le sentiment que l'ensemble des acteurs sont désormais conscients que ce genre d'attaques n'arrivent pas qu'aux autres, que chacun d'entre eux peut en subir.

Mme Mylène Jarossay. En synthèse, nous attendons une clarification sur la situation des entreprises françaises, leur éligibilité et une simplification des notifications d'incidents. Par ailleurs, une entreprise qui est victime d'une cyberattaque est déjà fortement impactée ; elle ne devrait pas subir la double peine

de la sanction. Il importe de bien réfléchir à cette question, la sanction doit servir à réparer et encourager une amélioration continue.

M. Arnaud Martin. Concernant la plateforme commune, nous soutenons l'idée de regrouper les propositions existantes. Nous avons déjà travaillé sur ce sujet avec certains de nos collègues, notamment le Clusif. Des graines ont déjà été semées ; nous sommes favorables à cette initiative.

M. Daniel Le Coguic. Deux aspects sont essentiels aux yeux de l'ACN : la collaboration entre acteurs nationaux, régionaux et publics ; et l'organisation de cette collaboration pour renforcer notre autonomie. La collaboration est ainsi essentielle, pour permettre à chacun de trouver sa place. C'est en établissant cette « équipe de France » du cyber que nous atteindrons les objectifs que la loi se donne en matière de résilience de la nation.

Ensuite, si nous ne maîtrisons pas les technologies de cybersécurité dans le numérique de demain, nous serons dépendants et notre résilience sera à géométrie variable. Si les solutions proviennent de France et de l'Union européenne, nous aurons accompli un pas de géant. Naturellement, nous n'atteindrons pas 70 % de parts de marché dans ce domaine, mais si nous parvenons à croître, tout le monde en sortira vainqueur ; les entreprises, le gouvernement, les régions.

Mme Bénédicte Pilliet. Au CyberCercle, nous estimons qu'en matière de cybersécurité, de sécurité numérique, rien ne peut être réalisé seuls. Ensemble, nous allons plus loin et plus vite ; nous avons besoin de collaborer. Les ressources existent en France, mais il est nécessaire de disposer d'objectifs communs et d'une organisation claire, pour offrir aux acteurs concernés par NIS 2 la lisibilité et la cohérence indispensables pour passer à l'action. Cela inclut la prise en compte des besoins et de la montée en compétence des acteurs régionaux et de leurs prestataires informatiques, qui les accompagnent au quotidien, dans le déploiement de NIS 2.

À ce titre, les référentiels et les labels nécessiteraient sans doute de mettre en place une réunion de concertation, qui permette d'inclure tous les acteurs dans une stratégie commune.

M. Jean-Noël de Galzain. De nombreuses initiatives existent déjà, mais il est crucial de poser un cadre général et de s'aligner sur une même direction, la transposition tenant lieu d'une forme de boussole, dans une approche systémique. Une fois le texte transposé, il est prévu de réécrire une stratégie nationale de cybersécurité, qui pourrait utilement intervenir dans le cadre du comité de filière, où nous convions tous les acteurs à participer. Nous aurons à cœur d'aligner la stratégie nationale de cybersécurité, afin de réussir ce passage vers la résilience générale. Il nous semble effectivement essentiel de réunir une « équipe de France » et d'y associer tous les acteurs de l'écosystème, dont le président du Campus cyber, le directeur général de l'Anssi, les représentants de cybermalveillance.gouv.fr.

Je confirme par ailleurs que le sujet de la cybersécurité intéresse désormais tout le monde. J'observe en outre que les jeunes générations sont particulièrement

sensibles au sujet de la protection des données. Je compte vraiment sur la représentation nationale pour garder en tête que la souveraineté doit être associée à toutes nos démarches dans le numérique ; il en va de notre autonomie stratégique.

Enfin, une collaboration entre public et privé est incontournable si nous voulons établir un modèle économique durable ; l'État ne peut pas tout faire seul. L'industrie prendra sa part, de manière coordonnée avec les autres parties prenantes. Nous produirons des efforts, comme nous le faisons tous les jours pour rendre la cybersécurité plus accessible et le numérique plus agréable à utiliser et plus sécurisé, à long terme.

M. Michel Dubois. Tout d'abord, je distingue deux niveaux de notification. Je ne pense pas qu'il soit nécessaire de légiférer sur le sujet des indicateurs de compromission (IOC), car des structures comme InterCERT en France permettent déjà aux CSIRT de partager ces informations. Le deuxième point concerne la notification vis-à-vis du régulateur. Je tiens à souligner l'importance d'avoir suffisamment de temps pour effectuer cette notification. Dans notre groupe, nous consacrons beaucoup de temps à vérifier les revendications de vol de données, car les pirates informatiques cherchent souvent à se vanter en réutilisant des données anciennes ou non pertinentes. Ce processus d'investigation est long et ne peut être accompli en seulement vingt-quatre heures. Enfin, j'insiste sur la nécessité d'harmoniser la procédure de notification, idéalement à travers une plateforme unique, par exemple portée par l'Anssi, qui diffuserait ensuite les informations aux différentes autorités compétentes, comme l'ACPR ou la Cnil.

En ce qui concerne les sanctions, il est crucial que tous les acteurs soient soumis au même régime. Plutôt qu'une simple sanction financière, pourquoi ne pas imposer l'achat de produits et de services de cybersécurité afin de se mettre aux normes ? Cela permettrait de rendre les sanctions à la fois plus constructives et cohérentes au niveau européen. En conclusion, je préconise un cadre législatif pragmatique et cohérent.

Mme Garance Mathias. Les labels peuvent offrir valorisation, attractivité et confiance. Le label, en tant qu'instrument juridique, doit avant tout inspirer confiance. Lors de l'élaboration du RGPD, cette notion n'avait pas été abordée, mais elle mérite d'être explorée aujourd'hui. Il est essentiel de considérer l'attractivité économique que peut générer la confiance. Au sein du Clusif, nous encourageons les échanges d'idées et le retour d'expérience des différents acteurs pour s'assurer que la loi s'aligne avec la réalité du terrain.

M. Sébastien Garnault. Je tiens d'abord à répondre à la demande de simplification administrative émise par M. le rapporteur général. Nos idées sont déjà sur la table, nous n'aurons donc pas besoin de soumettre un nouveau document. Concernant la stratégie nationale, il est crucial de définir clairement nos objectifs. La responsabilité politique et la continuité de l'engagement sont essentielles. Il est également important que les décrets d'application soient bien définis et que la vision ministérielle soit cohérente et continue.

M. le président Philippe Latombe. Je vous remercie pour vos interventions. Nous ne savons pas encore quand ce texte sera étudié dans l'hémicycle, probablement en septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer dans notre réflexion, éliminer des zones d'ombre, éviter les effets de bord et produire un texte le plus clair possible.

8. Table ronde réunissant des organisations patronales, jeudi 5 juin 2025 à 11 heures 30

Lors de sa deuxième réunion du jeudi 5 juin 2025, la commission spéciale a organisé une table ronde réunissant le Mouvement des entreprises de France (Medef) et Confédération des petites et moyennes entreprises (CPME).

M. le président Philippe Latombe. Nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde réunissant le Mouvement des entreprises de France (Medef) et la Confédération des petites et moyennes entreprises (CPME). Le Medef est représenté par Mme Rouilloux-Sicre, vice-présidente du groupe Thalès, présidente du comité régulation du numérique, Mme Briard, chargée de mission économie numérique, et Mme David, chargée de mission affaires publiques. Au titre de la CPME, nous accueillons M. Bataille, membre du comité exécutif de la CPME en charge du numérique et de l'innovation, M. Bothorel, référent cybersécurité, Mme Bouchet, juriste commerce et consommation et M. Dufour, responsable affaires publiques.

Une enquête menée en juin 2024 par l'Agence nationale de la sécurité des systèmes d'information (Anssi) auprès des membres du Clusif et mentionnée par nos collègues sénateurs dans leur rapport sur le projet de loi révèle qu'une cyberattaque coûte en moyenne 466 000 euros pour les très petites, petites et moyennes entreprises (TPE-PME), 13 millions d'euros pour les entreprises de taille intermédiaire (ETI) et 135 millions d'euros pour les grandes entreprises.

Une autre étude menée l'année dernière auprès de 500 TPE-PME pour le compte de cybermalveillance.gouv.fr sur leur niveau de maturité en matière de risque cyber montre que la situation est alarmante. Il en ressort que 61 % des entreprises françaises de moins de 250 salariés s'estiment faiblement protégées en matière de cybersécurité ou ne savent pas évaluer leur niveau de protection. Parmi les obstacles mentionnés pour atteindre le bon niveau de cybersécurité, la moitié des entreprises invoquent le manque de temps, le manque de connaissances et d'expertise, le manque de budget ou affirment encore ne pas savoir vers qui se tourner.

L'adoption de la directive NIS 2 et sa transposition par le titre II du projet de loi que la commission spéciale est chargée d'examiner constituent des réponses à l'augmentation de la cybercriminalité. Le projet de loi distingue deux catégories d'entités régulées, les entités essentielles et les entités importantes. Cette

catégorisation s'établit selon leur degré de criticité, leur taille et leur chiffre d'affaires. Selon l'Anssi, près de 2 000 entreprises privées devraient être considérées comme des entités essentielles.

Dans ce contexte, nous souhaitons vous entendre sur la manière dont vous percevez le projet de loi et sur les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du projet de loi par l'Assemblée nationale.

Mme Juliette Rouilloux-Sicre, vice-présidente du groupe Thales, présidente du comité régulation du numérique du Medef. Le Medef souhaite réaffirmer que ce texte, qui permet globalement d'élever le niveau de cybersécurité des entreprises françaises, est pertinent ; nous le soutenons. Les efforts de pédagogie conduits depuis maintenant un certain temps n'ont malheureusement pas suffi, face à la multiplication des attaques, notamment celles visant les PME-ETI.

Pour autant, le Medef est très attentif à éviter une surtransposition, pour plusieurs raisons. D'abord, la directive prévoit déjà un certain nombre d'obligations qui nous semblent suffire pour élever ce niveau de cybersécurité. Ensuite, il est important d'établir une harmonisation au niveau européen. Malheureusement, NIS 2 est une directive et non un règlement. Certains pays sont un peu plus en avance que la France dans leur transposition. Pour les entreprises implantées dans plusieurs pays européens ou celles qui visent des marchés européens, il est important de pouvoir disposer d'une certaine harmonisation des pratiques.

Il est également essentiel pour les entreprises de pouvoir disposer du texte définitif de transposition dans un délai raisonnable, qui permette également un travail parlementaire de qualité. Nous souhaitons également mentionner quelques points d'attention plus particuliers, notamment l'harmonisation des définitions. En effet, le texte en droit français n'adopte pas forcément la définition de la directive, ce qui est un peu regrettable.

Ensuite, les entreprises représentées par le Medef s'interrogent sur le champ d'application couvert par la notion « d'entités », qui suscite un certain nombre d'inquiétudes. En outre, les sanctions, très significatives, soulèvent également des craintes chez nos membres. Le Medef reconnaît la pertinence des sanctions, mais souligne leur nécessaire proportionnalité. Le texte doit également préciser que ces sanctions n'interviendront qu'en dernier recours. De plus, la sanction pénale du dirigeant ne nous semble pas forcément nécessaire, puisque les dirigeants d'entreprises agissent de la meilleure manière possible et qu'ils ne disposent pas forcément d'une grande expertise dans ce domaine.

M. Franck Bataille, membre du comité exécutif de la CPME, en charge du numérique et de l'innovation. La CPME représente plus de 243 000 entreprises et 5,5 millions de salariés. Le sujet qui nous réunit aujourd'hui engage l'avenir, la compétitivité et la sécurité de notre tissu économique. Membre du comité exécutif de la CPME en charge du numérique et de l'innovation, je dirige une petite entreprise de services numériques de dix personnes dans le Loir-et-Cher. À ce titre,

je connais bien la difficulté de la conformité en matière de cybersécurité pour des petites entreprises.

Je souhaite évoquer tout particulièrement le soutien aux objectifs de la loi et la responsabilité partagée. Nous souscrivons pleinement à l'ambition de rehausser le niveau de cybersécurité, tant pour protéger les entreprises que pour renforcer la résilience de notre pays. Nos adhérents sont conscients de la gravité croissante des menaces et souhaitent s'inscrire dans cette démarche.

Ensuite, je tiens à insister sur l'importance de la proportionnalité et de la non-surtransposition. Les travaux ont été menés dans un esprit d'équilibre et nous sommes satisfaits de ce point de vue, mais nous pointons l'attention sur la nécessaire progressivité, dans la mesure où toutes les structures n'ont pas forcément les mêmes moyens de mener à bien l'ensemble des actions, du jour au lendemain.

Les TPE et PME sont des entreprises pragmatiques, au contact de la réalité de l'économie de terrain. Un certain nombre d'exigences pèsent déjà sur elles et nous ne voudrions pas qu'elles fassent l'objet d'obligations et de contrôles ressentis comme disproportionnés et difficilement applicables d'une seule traite. Nous insistons donc sur la nécessité de leur accorder du temps et de les traiter de manière proportionnée.

Dans ces conditions, nous souhaitons travailler sur les éléments d'accompagnement, de pédagogie et de soutien opérationnel. Nous voulons avancer main dans la main avec vous, dans un esprit de confiance, de dialogue et de coconstruction. Nous soutiendrons les démarches qui favoriseront l'information, l'accompagnement, la proportionnalité, la tolérance, afin que la cybersécurité devienne un réflexe partagé, accessible à tous, mais également une source de compétitivité pour nos PME.

Mme Anne Le Hénanff, rapporteure. S'agissant des sanctions pénales du dirigeant, je tiens à rappeler que dans le cadre du règlement général sur la protection des données (RGPD) et de la fuite manifeste de données, la sanction pénale intervient s'il existe une preuve manifeste de non-volonté de se mettre en conformité. Il me semble que la directive NIS 2 partage le même esprit, mais nous pourrons en reparler si vous estimez que des précisions doivent être apportées dans le texte.

Que pensez-vous de l'idée, promue par certains acteurs, de rendre visible la démarche, voire l'atteinte, de la conformité à NIS 2 ? Que pensez-vous de l'idée d'une labellisation ?

Ensuite, j'aimerais connaître votre analyse sur les contrôles et les audits. Cet aspect suscite fréquemment des réactions, notamment de la part de ceux qui questionnent l'indépendance des organisations qui pourraient effectuer ces contrôles, voire qui souhaiteraient que celles-ci soient exclusivement françaises ou européennes. L'audit doit-il être généré par l'autorité de contrôle, l'Anssi, ou par l'entité elle-même concernée ? Comment appréhendez-vous cette thématique ?

Enfin, comment intégrez-vous la mise en conformité des 15 000 entités soumises à la directive NIS 2 vis-à-vis de leurs fournisseurs ou partenaires ? Estimez-vous que le contrat sera rempli lorsque les 15 000 entités se seront mises en conformité ou allez-vous plus loin, notamment vis-à-vis de la chaîne d'approvisionnement, en amont ou en aval ?

M. le président Philippe Latombe. Je partage les questions de Mme la rapporteure sur la labellisation et ses propos sur la sanction de l'intentionnalité. Certaines personnes qui ont été auditionnées promeuvent l'idée de la création d'un référent cyber au sein des entreprises, en mesure de s'adresser directement à l'organe dirigeant en cas de difficultés. Quel est votre point de vue à ce sujet, à la fois dans les grandes entreprises, mais aussi dans les PME et TPE ?

Ensuite, beaucoup souhaitent que le texte de loi fasse référence à des normes internationales existantes du type ISO 27000. Qu'en pensez-vous ? L'Anssi y est plutôt défavorable, mais d'autres pays ont opéré ce choix dans la transposition, notamment la Belgique.

Enfin, certaines personnes auditionnées pointent qu'un délai de notification d'une journée est trop court, car il est nécessaire de mener des investigations. Ils souhaiteraient pouvoir modifier ou moduler ce délai, avoir la capacité de pouvoir revenir sur des déclarations d'incidents ; lorsqu'ils sont moins graves qu'initialement redoutés, ou inversement. Comment envisagez-vous ce délai de notification ?

M. Marc Bothorel, référent cybersécurité, CPME. Tant que le règlement européen sur la cyber-résilience (Cyber Resilience Act, CRA) n'aura pas été mis en application par les différents fournisseurs et que les entreprises n'auront pas la possibilité de choisir un logiciel conforme au CRA, il apparaît difficile de sanctionner un chef d'entreprise qui se ferait attaquer au travers d'une chaîne logicielle.

Certaines PME sont directement assujetties à NIS 2, mais il leur faudra s'assurer que leurs sous-traitants proposent le même niveau de sécurité, même s'ils ne sont pas eux-mêmes assujettis. Dans le texte initial fourni par l'Anssi sur les vingt règles à mettre en œuvre et les entités capables de vérifier la mise en œuvre de ces mesures, figurent essentiellement des labellisés Anssi. Ils sont pourtant trop peu nombreux pour pouvoir traiter la masse des nouvelles sociétés qui seront soumises à cette réglementation.

Nous suggérons donc de s'appuyer sur les labellisés ExpertCyber, actuellement au nombre de 200 sur le territoire. Ces experts sont spécifiquement labellisés par l'Association française de normalisation (Afnor) pour traiter les TPE-PME. Ce label pourrait évoluer avec un volet spécifique dédié à la directive NIS 2, afin de vérifier la conformité à cette dernière des entités, des assujettis et donc de nos adhérents.

Pour l'aspect relatif aux sanctions, il faut considérer que certaines chaînes logicielles ne sont pas encore conformes au règlement européen sur la cyber-résilience, tant qu'il n'aura pas été mis en application. Ensuite, le sujet du référent NIS 2 est effectivement une bonne question. Cependant, sa mise en place semble compliquée. Dans les petites entreprises, le dirigeant pourrait assumer ce rôle, éventuellement aidé par un cabinet juridique.

M. Franck Bataille. Il y a trente ans, dans les TPE-PME, le point de contact sur les technologies de l'information était le comptable. Désormais, il s'agit du dirigeant. Obliger ces petites structures à disposer d'une personne spécifiquement formée à ces enjeux pourrait entraîner des coûts supplémentaires de recours à un prestataire externe, similaires à ceux engendrés par les délégués à la protection des données (DPO). Pour le niveau attendu du point de contact, tout dépendra des besoins de chaque entreprise, en fonction de sa taille. Une TPE de cinq personnes ne peut pas être tenue aux mêmes exigences qu'une PME de 200 personnes.

M. Marc Bothorel. Nous travaillons depuis deux ans, maintenant, avec l'Afnor sur une « Spec Afnor, dont l'objectif consiste à protéger les TPE-PME de 80 % des attaques les plus communes. Cette Spec est quasiment terminée et nous avons établi un groupe de travail, qui réunit notamment la direction générale des entreprises (DGE), l'Anssi, cybermalveillance.gouv.fr, les syndicats patronaux, les syndicats IT, BoostAeroSpace et La Poste. Cette Spec est rédigée et il ne nous reste plus qu'à traiter la labellisation des entreprises capables de vérifier sa conformité. J'ai d'ailleurs transmis le dossier à Clara Chappaz, la ministre déléguée chargée de l'intelligence artificielle et du numérique, et à l'Anssi. Nous estimons que la Spec Afnor peut être utile pour les sous-traitants, dans la mesure où elle comporte plusieurs niveaux (Silver, Gold et Platinum) et fournit un cadre de référence qui n'existe pas aujourd'hui.

Ensuite, une question a été posée concernant les délais de notification d'incidents. Un délai d'un jour paraît extrêmement court. Proposer un délai de soixante-douze heures, aligné sur les fuites de données pour la Commission nationale de l'informatique et des libertés (Cnil), pourrait être cohérent, car les incidents cyber et les fuites de données sont souvent concomitants.

Mme Anne Le Hénanff, rapporteure. Je me permets de vous rappeler que deux autres questions portent sur les organismes de contrôle nationaux et européens et sur l'affichage public de la mise en conformité.

M. Marc Bothorel. Une des missions d'un syndicat patronal consiste à diffuser l'information auprès des adhérents et les inciter à se mettre en conformité. À ce sujet, l'Anssi compte sur nous. Il ne faut pas rééditer la même erreur que pour le RGPD et ne parler de la directive NIS 2 que sous l'aspect des sanctions, mais bien valoriser la conformité comme un atout commercial, celui d'être considéré comme un « partenaire de confiance ».

Mme Juliette Rouilloux-Sicre. La rédaction actuelle sur les sanctions mérite sans doute d'être affinée, pour correspondre à l'état d'esprit qu'évoquait Mme la rapporteure.

Le label de conformité doit être bien encadré pour éviter des autodéclarations subjectives. Un vrai cahier des charges est donc nécessaire, en laissant du temps aux entreprises pour se mettre en conformité. En effet, le degré de maturité cyber n'est pas le même selon la taille de l'entreprise. Dans ce cadre, l'Anssi semble désignée pour octroyer ce label en tant qu'entité de confiance, mais sera sans doute confrontée à une problématique de moyens. Quoi qu'il en soit, le label permettrait à tous, y compris aux citoyens, de connaître le niveau de conformité.

La conformité doit aussi être envisagée comme une opportunité de développement des affaires : le Medef considère qu'une entreprise responsable s'orientera plus naturellement vers un prestataire conforme.

Nous comprenons la logique des contrôles et des audits. Les contrôles, internes ou externes, sont essentiels, mais il convient de veiller à ce que les prestataires qui offriront des services soient bien compétents. Le Medef ne voit aucun obstacle à des contrôles effectués par l'Anssi, mais fait preuve de vigilance sur d'éventuels conflits d'intérêts si des tiers interviennent. Dans quelles conditions agiront-ils ? Quels seront les critères de sélection ? En effet, un auditeur pénètre au cœur des systèmes et peut accéder potentiellement à un certain nombre de failles. La même vigilance concerne les éléments de souveraineté.

Ensuite, dans le cadre de la directive NIS 1, il est parfois difficile pour les entreprises de transférer leurs exigences aux fournisseurs et prestataires. En revanche, nous estimons que NIS 2 peut offrir une opportunité, dans la mesure où elle concernera un bien plus grand nombre d'entreprises. De fait, la prise de conscience des entreprises sur la cybersécurité sera rehaussée avec cette réglementation. Pour autant, la démarche sera complexe, raison pour laquelle nous sommes vigilants en termes de surtransposition : il ne faudrait pas imposer à des fournisseurs sous-traitants de taille plus modeste des exigences qu'ils ne pourraient pas tenir.

À ce titre, il faut veiller à établir une harmonisation au niveau européen, dans la mesure où les fournisseurs et sous-traitants français ne travaillent pas toujours uniquement avec des entreprises françaises. Je pense notamment aux ETI ou aux PME, qui ont moins de moyens, moins de capacités à se mettre en conformité.

Ensuite, le rôle de référent cyber nous semble effectivement constituer une bonne idée, mais il ne devrait pas nécessairement être tenu par le responsable de la sécurité des systèmes d'information (RSSI), qui pourrait être considéré comme juge et partie. Dans la mesure où il s'agit d'un sujet de conformité, cette tâche pourrait être assurée par le directeur juridique. Le Medef recommande depuis longtemps une

montée en compétences sur ces sujets cyber, pour l'ensemble du tissu industriel français. À cet égard, des efforts de formation devraient être accomplis, mais à moindre échelle, puisque la cybersécurité est désormais mieux connue.

Utiliser des normes internationales comme ISO ou celles en cours de développement par l'Afnor est bénéfique, mais il est crucial que ces normes s'appliquent uniformément à tous. En effet, la directive NIS 2 implique une responsabilité qu'il ne faut pas restreindre uniquement aux grandes entreprises, au risque de créer des « trous dans la raquette ». Je rappelle ainsi que l'objectif initial de la directive consistait bien à s'assurer d'un bon niveau de cybersécurité en Europe. Ceci est d'autant plus important que les attaques sont aujourd'hui très variées ; elles touchent tous les secteurs d'activité et toutes les tailles d'entreprise.

Vous avez également mentionné les délais de notification. À ce titre, il convient de distinguer les fuites de données personnelles, qui font l'objet de déclarations à la Cnil, et les fuites de données industrielles. Dès lors, il n'est pas forcément pertinent d'intégrer dans le texte une déclaration d'office à la Cnil en cas d'incident cyber au titre de NIS 2, puisqu'un incident cyber ne donne pas forcément lieu, heureusement, à une fuite de données personnelles.

Le délai de vingt-quatre heures ne pose pas de problème au Medef, dès lors qu'il concerne une première notification. En revanche, il importe sans doute d'apporter une clarification concernant le type d'incident de cybersécurité qu'il convient de déclarer, dans la mesure où plusieurs dizaines de milliers d'incidents cyber interviennent chaque jour. Nous relevons avec satisfaction que la nouvelle version du texte apporte d'ailleurs une amélioration en ce sens. À l'inverse, un délai de soixante-douze heures peut sembler long : de nombreuses données peuvent avoir fui, des systèmes être bloqués. En conséquence, il peut être très utile pour une ETI d'obtenir le soutien de l'Anssi dans un délai plus rapide.

Nous sommes en revanche favorables à l'établissement d'un formulaire unique et, idéalement, d'un guichet unique, qui pourrait être assuré par l'Anssi, laquelle pourrait coordonner les déclarations et assurer la conformité. Or la rédaction actuelle du texte ne prévoit pas cette possibilité.

Enfin, je souligne que diverses autorités sectorielles mettent également en place des dispositifs en matière de cybersécurité.

M. Marc Bothorel. NIS 2 formule des exigences en matière de formation des utilisateurs. Aujourd'hui, nos adhérents cotisent aux fonds professionnels, les opérateurs de compétences (Opco) tous les mois de février, mais ne dépensent pas nécessairement leur budget. S'il ne s'agit pas d'une formation certifiante, elle constitue malgré tout la première ligne de défense d'une entreprise et désormais une exigence des assurances cyber. Ne serait-il pas envisageable de prendre en charge ces sensibilisations annuelles dans le cadre des Opco ? Compte tenu du contexte économique et géopolitique, cela mettrait le pied à l'étrier à des chefs d'entreprise pour la formation de leurs employés, de manière annuelle.

S'agissant des autorités de contrôle, vous avez évoqué ISO 27001. Cependant, pour une PME de cinquante personnes, le coût d'une conformité ISO 27001 est hors de portée. À ce propos, je me permets de rappeler une décision du tribunal d'appel de Rennes, qui a condamné un sous-traitant pour manquement à son devoir de conseil auprès d'une entreprise qui a subi une cyberattaque. Cette décision fera vraisemblablement jurisprudence. De fait, les prestataires IT ont tout intérêt à effectuer leur métier de la manière la plus rigoureuse, dans le cadre de NIS 2.

M. le président Philippe Latombe. La directive NIS 2 prévoit que l'Anssi élabore un référentiel qui ne figure pas dans le texte de loi, mais prendra la forme d'un décret en Conseil d'État. Cela vous pose-t-il un problème d'instabilité juridique, de visibilité et de prévisibilité ?

De leur côté, un certain nombre de pays européens ayant déjà transposé ont pleinement utilisé les considérants de la directive, en estimant qu'il fallait le plus possible faire référence à des normes internationales, de type ISO 27001. Les législateurs belges ont ainsi inscrit dans le texte de loi une référence directe à de telles normes internationales. Faut-il en faire autant où maintenir une forme de souplesse, ainsi que l'Anssi le suggère ?

Mme Juliette Rouilloux-Sicre. Certains pays ont inclus des termes comme « *notamment* » ou « *de type* », créant ainsi de l'insécurité juridique. Le Medef n'est pas opposé à une définition du référentiel après la promulgation de la loi, tant que cela ne prend pas trop de temps. La transposition de la directive en droit français a pris plus de temps que prévu, même si cela permet de conduire des consultations, comme celle à laquelle vous nous permettez de participer. Cependant, le texte prévoit de nombreux renvois à des décrets en Conseil d'État, s'agissant notamment du référentiel. Or nous redoutons que ces décrets tardent à être publiés, d'autant plus que l'Anssi dispose de ressources limitées. Par ailleurs, il n'y a pas de délai de mise en conformité : en théorie, les entreprises devront être conformes immédiatement, d'un strict point de vue juridique.

Nous recommandons que le référentiel soit rapidement établi et qu'il ne s'éloigne pas trop des standards internationaux. Nous sommes préoccupés par la façon dont les entreprises choisiront leurs prestataires sans critères clairs. Il est important que la mise en place du référentiel prenne en compte les spécificités françaises tout en restant alignée avec les normes internationales.

M. Franck Bataille. Nous ne sommes pas non plus pas opposés à une définition du référentiel après la promulgation de la loi, sous réserve qu'elle intervienne rapidement. Il ne faudrait pas non plus qu'il soit inapplicable pour les TPE et PME. En effet, un référentiel trop pointu ne pourrait pas être mis en œuvre par ces dernières. Il faut tenir compte des réalités de terrain. À titre d'exemple, dans mon petit département du Loir-et-Cher, 80 % de mes adhérents ont encore une adresse wanadoo.fr. Il sera très compliqué de leur faire sauter plusieurs marches du jour au lendemain. Nous plaidons donc en faveur d'une démarche progressive dans

le cadre d'un référentiel, qui doit être appliqué différemment en fonction de la dimension des entreprises.

M. Marc Bothorel. Je complète ces propos concernant la déclaration de l'incident. En tant que réserviste à l'Unité nationale cyber, je souhaite mettre en lumière une problématique sur laquelle nous avons travaillé. Certaines petites entreprises ont tenté de faire des demandes auprès de l'Anssi, bien que ce ne soit pas son rôle pour des sociétés d'environ cinquante personnes : elle traite principalement d'acteurs de plus grande taille, appelés opérateurs de services essentiels (OSE) et opérateurs d'importance vitale (OIV), dans l'ancienne nomenclature.

Il est donc pertinent de souligner l'importance du numéro 17Cyber, qui a été créé pour fournir une permanence gendarmerie-police, vingt-quatre heures sur vingt-quatre et sept jours sur sept, capable d'aider les petites entreprises dans leurs déclarations d'incident. Des retours du terrain, notamment de brigades de gendarmerie, montrent que certains chefs d'entreprise n'ont pu déposer plainte faute de spécialistes présents.

Le mécanisme mis en place depuis le 17 décembre dernier constitue une solution appropriée pour les PME. Il permet à ces entreprises de bénéficier d'un support adapté pour toutes leurs déclarations d'incident, contrairement à l'Anssi qui ne traite pas les cas des PME de cette taille.

Mme Juliette Rouilloux-Sicre. L'Anssi a déjà fait circuler quelques versions de son référentiel et une nouvelle version sera bientôt disponible. Inspirés par des secteurs comme l'aéronautique, où Boost Aerospace utilise des niveaux de conformité (Silver, Gold et Platinum), nous pourrions envisager un référentiel similaire. Celui-ci tiendrait compte de la criticité des activités confiées aux sous-traitants et prestataires.

J'insiste à mon tour sur le caractère crucial des délais. Il est impératif que ce référentiel soit publié rapidement. Les entreprises ont besoin de clarté pour mettre en œuvre les directives, estimer les coûts et ajuster leurs offres en conséquence. Pour le moment, elles attendent.

Mme Anne Le Hénanff, rapporteure. Je tiens à réagir en ce qui concerne les décrets, pour partager l'opinion qui vient d'être exprimée. À titre d'exemple la loi visant à sécuriser et à réguler l'espace numérique (loi Sren) date de l'année dernière. Pourtant, sur la partie *cloud* que je portais, 80 % des décrets n'ont toujours pas été publiés. Il sera donc utile de transmettre ce message à Mme la ministre, que nous auditionnerons prochainement.

Ensuite, je souhaite vous poser deux questions concernant l'accompagnement, étant donné que vous représentez des fédérations professionnelles. Premièrement, envisagez-vous de mettre en place des campagnes ou des actions visant à sensibiliser vos membres, notamment pour éviter les effets d'aubaine des offres commerciales proposées par des cabinets profitant de textes

non encore publiés ? Depuis déjà un an, certains vendent des services de mise en conformité avec NIS 2 alors même que le texte n'est pas encore sorti. Comment comptez-vous sensibiliser vos membres à ce sujet ?

Deuxièmement, envisagez-vous d'identifier activement vos ressortissants concernés par NIS 2, ou les laisserez-vous se déclarer eux-mêmes à l'Anssi ? J'aimerais comprendre comment vous intégrez ces éléments dans vos stratégies de communication.

M. Marc Bothorel. Nous avons également organisé des réunions avec l'Anssi sur ce sujet et sommes quelque peu déçus de la manière dont l'Anssi nous délègue cette responsabilité. Le dernier message reçu indiquait en substance : « *Nous n'avons pas de support de présentation à vous fournir, débrouillez-vous et faites de la publicité auprès de vos adhérents* ».

Au-delà, le seul outil disponible, « MonEspaceNIS2 », est toujours en phase bêta pour la partie relative à la qualification. Un autre point préoccupant concerne l'absence d'étude d'impact, ce qui nous empêche d'informer nos adhérents sur le temps et le coût nécessaires à la mise en conformité. Cela est extrêmement regrettable. Nous avons d'ailleurs déjà évoqué ce sujet auprès de Vincent Strubel, le directeur général de l'Anssi.

M. Franck Bataille. Pour répondre à votre question sur l'effet d'aubaine, nous avons déjà travaillé sur ce sujet, que ce soit pour NIS 2 ou pour le RGPD. Nous avons relayé des messages indiquant que les plateformes en ligne qui promettent monts et merveilles ne reflètent pas la réalité. Nous sommes également vigilants sur l'arrêt du cuivre, qui crée des opportunités pour certains, mais peut induire en erreur nos TPE et PME avec des offres non pertinentes ou viables. Nous continuons d'expliquer ces aspects à nos membres, tout comme le font les associations locales dans leurs collectivités. Nous veillons régulièrement à ce que nos unions territoriales portent également ce message.

M. Marc Bothorel. Nos adhérents ne sont pas des spécialistes. Nous attendions de l'Anssi que l'ensemble des règles techniques qui ont été édictées soient établies de manière plus compréhensible. En effet, elles s'adressent essentiellement à des directeurs des services informatiques (DSI) et des RSSI. J'ai récemment eu l'occasion d'en discuter avec le Clusif et nous partageons le même point de vue à cet égard : une approche progressive serait clairement bénéfique.

Cette progressivité doit aussi s'inscrire dans une démarche de bienveillance pendant le temps de la mise en place, en prenant en considération la situation économique et géopolitique, ainsi que les problématiques de trésorerie auxquelles les entreprises sont aujourd'hui confrontées. Le coût de mise en œuvre initiale de NIS 2, sans parler des coûts annuels récurrents, impactera fortement la trésorerie des petites entreprises. Il est donc nécessaire d'établir une période de bienveillance et d'accompagnement de la part de l'Anssi et de l'écosystème, ainsi qu'une écriture des règles à mettre en œuvre de manière progressive, à partir d'un socle sur lequel

sera progressivement construit l'ensemble des règles et des obligations de NIS 2. Actuellement, les vingt règles sont posées d'un coup, et il incombe aux utilisateurs de décrypter leur contenu, ce qui n'est pas toujours simple pour un non-spécialiste.

M. le président Philippe Latombe. Nous avons souhaité, comme l'a exprimé le rapporteur général, organiser une première audition avec le directeur général de l'Anssi. Nous le réauditionnerons une dernière fois après toutes les auditions, pour revoir les points soulevés et envisager éventuellement des évolutions. Ensuite, nous auditionnerons en dernier la ministre qui portera le texte, ce qui servira de base à notre discussion générale pour la commission. À ce titre, les messages que vous nous adressez aujourd'hui sont nécessaires pour les deux auditions à venir. Les auditions publiques permettent précisément d'élargir le spectre du débat.

Mme Juliette Rouilloux-Sicre. Le Medef a pour habitude d'accompagner ses adhérents et le débat sur la cybersécurité n'y déroge pas. Une fois que le texte aura été publié, nous agirons en ce sens de manière encore plus poussée, en essayant de faire œuvre de pédagogie. À ce sujet, nous souhaiterions pouvoir disposer de documents standards, que chaque organisation pourrait diffuser de la même manière au sein de ses fédérations. Mais nous n'avons pas attendu pour agir. Une équipe numérique du Medef y travaille, y compris sous la forme de webinaires.

Le Medef croit beaucoup à la cybersécurité et estime qu'il s'agit d'un point fort en termes de souveraineté. Encore une fois, avoir des documents standardisés aiderait à assurer la bonne compréhension et à éviter les mauvaises interprétations.

Sur le sujet de l'identification des entreprises, le Medef ne prendra pas la responsabilité, car elle incombe à l'entreprise elle-même. NIS 2 prévoit d'ailleurs une charge de la preuve un peu différente par rapport à NIS 1. Les entreprises doivent s'identifier, faire leur propre auto-évaluation et déterminer si elles sont une entité essentielle, importante ou non concernée. Nos adhérents demandent un accompagnement plus prononcé de l'Anssi sur le sujet, qui tarde pour le moment, pour des raisons que nous comprenons par ailleurs, tant elle doit couvrir un grand nombre de secteurs et d'entreprises.

Il n'en demeure pas moins que nombre d'entreprises aimeraient un accompagnement plus marqué de l'Anssi sur la qualification, pour pouvoir s'assurer qu'elles ont choisi la bonne. De fait, dans leur très grande majorité, les entreprises font preuve d'une très bonne volonté, ont envie de se mettre en conformité. Mais parfois, leur niveau de maturité cyber n'est pas encore excellent.

Je me permets également de revenir sur un point abordé lors de mon exposé liminaire. Il est important d'utiliser un vocabulaire cohérent dans le texte de transposition, afin d'éviter les différences de définition entre le droit français et la directive. Pour les groupes ayant des entités dans plusieurs pays européens, il faudrait envisager un guichet unique. En effet, contrairement au RGPD, NIS 2

manque d'un tel outil, ce qui complique la gestion des incidents pour les grandes entreprises multinationales.

La directive NIS 2 complique la tâche de deux types d'entreprises. Il s'agit d'une part des petites et moyennes entreprises, parce qu'elles ne connaissent pas très bien le cyber. Il s'agit d'autre part des grands groupes, présents dans un certain nombre de pays européens et dont les qualifications sont parfois différentes selon les pays, selon la transposition qui a été opérée en droit national. En conséquence, ils doivent notifier et se déclarer auprès de plusieurs autorités de contrôle.

En résumé, il serait opportun que le législateur français prête une attention particulière aux terminologies utilisées et que l'Anssi puisse jouer un rôle de guichet unique et fournir un support.

M. le président Philippe Latombe. Il existe effectivement une forte demande de la part des entreprises, quel que soit leur secteur. Souhaitez-vous aborder d'autres points ?

M. Marc Bothorel. Je souhaite revenir sur la nécessité d'un accompagnement budgétaire pour aider nos adhérents à se mettre en conformité dans un domaine, qui n'est pas aujourd'hui perçu comme un outil de productivité. Actuellement, nous constatons le « saupoudrage » des différents budgets accessibles, sujet que nous avons déjà abordé devant la commission sénatoriale. À cette occasion, j'avais pris l'exemple d'une petite entreprise implantée dans la « diagonale du vide » qui serait soumise à NIS 2, sans prestataire à proximité, sans faculté d'accéder à des budgets.

Il est donc essentiel d'assurer une égalité de traitement et d'accessibilité aux budgets accompagnant les PME pour se mettre en conformité.

Malheureusement, cela n'est pas le cas aujourd'hui. Dorothée Decrop, déléguée générale d'Hexatrust, que vous avez reçue un peu plus tôt ce matin, réalise un travail formidable pour essayer d'identifier les différentes sources de budgets disponibles auprès des entreprises. Mais au-delà de l'identification, l'essentiel consiste surtout à pouvoir accéder à ces budgets. Or il existe de très fortes distorsions dans ce domaine. À titre d'exemple, en Île-de-France, le budget de 10 millions d'euros mobilisé par le conseil régional pour les PME n'était accessible qu'aux entités labellisées « prestataire d'audit de la sécurité des systèmes d'information » (Passi) par l'Anssi, dont les coûts par journée étaient trop élevés pour des budgets de PME.

Si nous voulons réussir la mise en œuvre de NIS 2, il faut introduire de la rationalité, à la fois sur la capacité de nos adhérents à accéder effectivement à des prestataires capables de les mettre en conformité, mais également à des accompagnements budgétaires pour la mise en conformité. Lorsqu'internet s'était diffusé, dans les années 2000, une loi de finances avait inscrit un crédit d'impôt de 50 % pour s'équiper en équipements réseau et ainsi accéder à internet. Ne pourrait-on pas imaginer un dispositif similaire ?

Toutes choses égales par ailleurs, un investissement de l'État pour aider les entreprises à se protéger lui coûterait moins cher que les conséquences d'attaques cyber sur celles-ci, qui se traduiraient par des dépôts de bilan, des mesures de redressement, des recettes fiscales en moins et des chômeurs supplémentaires, qu'il faudrait indemniser.

M. Franck Bataille. Dans certaines régions, comme le Loir-et-Cher, la complexité et la multiplicité des dispositifs peuvent retarder considérablement la mise en place de mesures de cybersécurité. Dans mon département, j'ai le souvenir d'un adhérent, employeur de soixante salariés qui voulait mettre en place différentes mesures de cybersécurité. Il lui a fallu plus d'un an pour aller au bout de la démarche. Il arrive qu'un plus grand nombre de ressources soient dépensées pour préparer les dossiers de demande d'aides que pour bénéficier réellement de ces aides. Simplifier et améliorer l'efficacité de ces dispositifs pourrait grandement aider les PME.

M. le président Philippe Latombe. Ce type de questions sera abordé avec Mme la ministre, même si elles relèvent plus de la loi de finances que d'un texte de cet ordre.

Ensuite, nous avons longuement évoqué aujourd'hui les sanctions de nature pénale. En revanche, je suis surpris qu'aucun de vous n'ait mentionné le fait que seules les entreprises étaient soumises à une possibilité de sanction alors que le secteur public n'est pas concerné. Quel est votre point de vue à ce sujet ?

Je souhaite enfin vous poser une question au nom notre collègue Mickaël Bouloux, rapporteur en charge de la partie relative à la directive Dora. Avez-vous identifié des zones de frottement, des incompatibilités, entre la directive NIS 2 et Dora qui justifieraient des modifications du texte de transposition, pour le rendre cohérent ? En effet, selon diverses personnes auditionnées, Dora prévoit que les entreprises assujetties à la directive puissent diligenter des audits auprès de leurs sous-traitants. Deux remarques ont été formulées à ce propos. D'une part, la durée et le coût de ces audits ne sont pas détaillés. D'autre part, cette question soulève des préoccupations concernant l'accès potentiel à des informations sensibles par des cabinets étrangers. Ce sujet vous préoccupe-t-il ? Avez-vous des recommandations à formuler à ce propos ?

Mme Juliette Rouilloux-Sicre. Pour le Medef, la disproportion un peu systématique sur ces sujets de conformité entre les entités publiques et les entreprises ne semble pas pertinente. Actuellement, le niveau de cybersécurité des collectivités est parfois bas, ce qui peut s'expliquer par différentes raisons. Elles sont soumises à d'autres types de demandes de la part des citoyens, qui ne portent pas vraiment sur le cyber, mais plutôt sur des préoccupations plus classiques comme la qualité des équipements, le bon fonctionnement des écoles.

Néanmoins, nous redoutons qu'en l'absence de sanctions, ces collectivités ne prennent pas ce sujet à bras-le-corps et ne le traitent pas avec autant diligence

que les entreprises, alors même qu'elles ont accès à un certain nombre de données importantes pour le secteur privé. Les entreprises leur communiquent par exemple des données qui sont parfois sensibles. Il nous semble important que l'ensemble de l'écosystème français se mette en conformité, même s'il ne revient pas au Medef de prôner telle ou telle sanction pour les administrations ; notre organisation défend les entreprises.

En revanche, nous considérons que le montant des sanctions est extrêmement élevé et que leur assiette de calcul n'est pas complètement claire, notamment pour les groupes d'entreprises. Ces sanctions sont ainsi déterminées par rapport au chiffre d'affaires. Mais de quel chiffre d'affaires est-il question ? S'agit-il de celui de l'entité qui a commis une négligence ou de celui du groupe en entier ? Le Medef préfère évidemment la première possibilité, dans la mesure où un groupe n'est pas forcément informé de ce qui se passe dans l'une des entités. Par ailleurs, nous considérons que le montant des sanctions est effectivement très significatif ; elles peuvent mettre en péril l'activité des entreprises. Nous avons compris que la mise en œuvre serait effectuée avec une certaine bienveillance, mais le Medef est très vigilant à ce sujet.

Ensuite, vous avez mentionné les craintes liées à la conduite des audits par des cabinets étrangers. Compte tenu de la responsabilité qui pèse sur les donneurs d'ordre dans le cadre de NIS 2, il nous semble utile qu'ils puissent mener des audits auprès de leurs sous-traitants et fournisseurs. Cela permet effectivement de vérifier la conformité sur des activités critiques pour la nation et certains secteurs. En revanche, ces contrôles et audits doivent être conduits par des entreprises labellisées. Il existe déjà un certain nombre de labellisations cyber.

Le texte prévoit également la possibilité pour les autorités d'échanger avec des organismes internationaux qui œuvrent dans le domaine de la cybersécurité. En revanche, ni la directive NIS 2, ni le texte de transposition ne fournissent de détails. Le Medef souhaite s'assurer que des informations confidentielles, y compris celles liées au secret des affaires, ne soient pas transmises à des tiers dans le cadre de discussions internationales.

Enfin, en matière de normes, le Medef préfère des normes internationales établies plutôt que des normes très spécifiques et sectorielles : nous préférons une norme ISO à une norme Afnor, car elle nous semble plus correspondre à l'objectif d'harmonisation.

M. Franck Bataille. Nos territoires sont très impliqués dans le développement économique. Les relations de la CPME avec les collectivités territoriales sont extrêmement fréquentes. Nous partageons avec elles un grand nombre d'informations, parfois stratégiques. Quelle que soit la taille des entreprises, nous sommes dans une relation de confiance, notamment concernant les informations que nous leur confions. De fait, les collectivités sont très souvent les premières informées de nos projets économiques, comme la construction de bâtiments. Nous croyons en leur accompagnement, en leur bienveillance et en leur

aide, et nous ne voudrions pas que les informations que nous transférons soient dispersées ou fassent l'objet de fuites. C'est la raison pour laquelle les acteurs publics devraient aussi porter, selon nous, leur part de responsabilité, de la même manière que les collectivités locales sont aujourd'hui responsables en matière de RGPD.

Ces collectivités territoriales sont des partenaires, au même titre que l'ensemble de notre chaîne d'approvisionnement, elles font aussi partie de l'écosystème. Elles partagent également un certain retard dans l'appréhension des enjeux cyber, au même titre que les TPE et PME. Je le sais d'autant mieux que j'ai été sollicité la semaine dernière pour intervenir lors d'un congrès de maires de petites communes dans mon département, au titre d'expert cyber. Un grand travail reste à accomplir vis-à-vis de ces acteurs territoriaux, qu'il faudra aussi responsabiliser.

M. Marc Bothorel. S'agissant de la responsabilité du chef d'entreprise, nous avions déposé un amendement, qui avait été accepté, auprès de la commission sénatoriale, en faveur d'une proportionnalité en fonction de la gravité du manquement. Cette mesure vise à éviter des sanctions trop lourdes qui pourraient mettre en difficulté des entreprises.

Enfin, je souhaite vous faire part d'un exemple pour illustrer les difficultés auxquelles nous sommes confrontés pour transmettre les messages et informations. Nous avions organisé en Ardèche une réunion d'information conjointe avec la chambre de commerce, la préfecture, une importante communauté de communes, la gendarmerie et le conseil départemental au sujet de NIS 2, à destination des entreprises. Cet événement, qui devait se dérouler le 12 juin, vient d'être annulé. Seulement six personnes s'étaient inscrites.

M. le président Philippe Latombe. Je vous remercie. Nous ne savons pas encore quand ce texte sera étudié dans l'hémicycle, probablement en septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer à notre réflexion et produire un texte le plus lisible et efficace possible. L'objectif consiste en effet à éviter des zones d'ombre et des effets de bord.

9. Audition de représentants de la Commission nationale de l'informatique et des libertés (CNIL), mardi 10 juin 2025 à 16 heures 30

Lors de sa réunion du mardi 10 juin 2025, la commission spéciale a auditionné M. Michel Combot, directeur des technologies, de l'innovation, et de l'intelligence artificielle, M. Victor Nicolle, directeur des contrôles et des sanctions, M. Florent Della Valle, chef du service de l'expertise technologique et Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles, représentant la Commission nationale de l'informatique et des libertés (CNIL).

M. le président Philippe Latombe. Nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, avec l'audition de représentants de la Commission nationale de l'informatique et des libertés (Cnil).

À titre liminaire et à toutes fins utiles, je tiens à indiquer que je suis membre du collège de la Cnil.

Le projet de loi que la commission spéciale est chargée d'examiner comporte trois titres. Le titre Ier, consacré à la résilience des activités d'importance vitale, procède à la transposition de la directive sur la résilience des entités critique, dite REC. Mme Catherine Hervieu en est la rapporteure. Le titre II vise à renforcer notre cadre juridique en matière de cybersécurité et procède à la transposition de la directive européenne NIS 2 (*Network and Information Security* 2). Mme Anne Le Hénanff en est la rapporteure. Enfin, le titre III est consacré à la résilience opérationnelle numérique du secteur financier et procède à la transposition du règlement sur la résilience opérationnelle numérique du secteur financier, dit Dora (Digital Operational Resilience Act). M. Mickaël Bouloux en est le rapporteur. Éric Bothorel est le rapporteur général du projet de loi.

Plusieurs dispositions du projet de loi sont relatives à la Cnil.

L'article 17 dispose que l'Agence nationale de la sécurité des systèmes d'information (Anssi) informe la Cnil des incidents ayant un impact important sur la fourniture des services des entités essentielles et importantes ainsi que de certaines administrations, et susceptibles d'entraîner une violation de données à caractère personnel. Cette notification permettra à la Cnil d'exercer ses missions de contrôle et de sanction, conformément au Règlement général sur la protection des données (RGPD).

Les articles 19 et 22 sur les données relatives aux noms de domaine renvoient leurs modalités d'application à deux décrets en Conseil d'État, pris après avis de la Cnil.

L'article 23 encadre les échanges d'informations, notamment entre l'Anssi et la Cnil.

Enfin, l'article 37, alinéa 5, dispose que si les manquements relevés dans le cadre du titre II constituent également une violation du RGPD donnant lieu à une amende administrative prononcée par la Cnil, la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative. Cette disposition suscite des interrogations, non sur le principe bien connu du *non bis in idem,* mais sur les modalités d'application concrètes des procédures et sur leur articulation.

Dans ce contexte, nous souhaitons vous entendre sur la manière dont vous percevez le projet de loi et sur les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du texte par l'Assemblée nationale. Je vous

laisse la parole pour une intervention liminaire, avant que nos rapporteurs et l'ensemble de nos collègues puissent vous interroger.

M. Michel Combot, directeur des technologies, de l'innovation et de l'intelligence artificielle de la Cnil. Merci, monsieur le président, de nous donner l'occasion de nous exprimer sur ce projet de loi, lié au cœur des activités de la Cnil en matière de cybersécurité.

La Cnil doit veiller au respect de la vie privée et au développement des innovations et des nouveaux services. L'enjeu de la cybersécurité constitue l'une des priorités de la Commission, dont la prérogative principale en la matière est la gestion des incidents liés aux violations de données. Depuis 2018, en application du RGPD, les entreprises ont l'obligation de notifier vols et pertes de données à la Cnil, qui instruit ces incidents et considère, le cas échéant, si les entreprises ont bien appliqué certaines dispositions.

L'augmentation des incidents liés à la cybersécurité s'est traduite par une augmentation des violations de données, dont le nombre a été supérieur à 5 500 en 2024. Plus de 50 % de ces violations sont liées à des actes de piratage, soit des actes volontaires extérieurs, et près de 45 % sont liées à des problèmes rencontrés par l'entreprise. Par ailleurs, plus d'un tiers des incidents concernent des PME.

Du point de vue de la Cnil, le renforcement de la maturité des entreprises dans le domaine de la cybersécurité constitue un enjeu clé, notamment pour la protection des données personnelles détenues par les entreprises. À cet égard, la Cnil ne peut que soutenir l'objectif initial de la directive NIS 2 et de sa transposition dans le droit français. Plus les entreprises seront préparées, mieux elles seront à même de protéger les données de leurs clients et la vie privée de nos concitoyens.

La Cnil accompagne aussi de manière globale le secteur, en édictant les obligations dérivées du RGPD en matière de cybersécurité. À titre d'exemple, en ce qui concerne l'authentification multifacteurs, l'accès en interne doit être très sécurisé pour les grandes bases de données. Nous avons développé un programme de travail pour nous assurer que les bonnes pratiques sont appliquées par les entreprises, en ciblant des secteurs et des tailles d'entreprises correspondants aux violations de données constatées. La cybersécurité est l'une des priorités de notre plan d'action 2025-2028. L'un des enjeux sera d'intégrer les collectivités locales dans le champ des obligations dérivées de la directive NIS 2.

J'en viens au projet de loi, dont l'architecture nous convient. L'articulation de nos activités avec celles de l'Anssi constitue un enjeu. Cependant, nous collaborons déjà au quotidien depuis la création de l'Agence à la fin des années 2000. Cette question de l'articulation se pose pour plusieurs sujets, dont certains font l'objet d'articles du projet de loi et d'autres d'un travail opérationnel.

La transposition de la directive NIS 2 va décupler le nombre d'entreprises concernées par les exigences et les obligations en matière de cybersécurité. À cet

égard, un minimum doit être mis en place quant à la protection des données personnelles, en l'adaptant à la capacité des entreprises. L'Anssi travaille à ce calibrage et nous collaborons très bien à ce stade. Le niveau de maturité des entreprises, en particulier les plus petites, et des collectivités locales s'en trouvera amélioré.

J'en viens au sujet de la notification. Le projet de loi prévoit que l'Anssi doit informer la Cnil de certains incidents, ce qui nous convient parfaitement. Pour nous, l'enjeu est d'agir le plus rapidement possible. La notification des violations de données permet d'abord d'informer les concitoyens touchés, afin de prévenir toute fraude ultérieure. La divulgation d'informations, notamment bancaires, peut se révéler très préjudiciable, en particulier pour les populations les plus défavorisées, moins enclines à identifier ce genre de fraudes. Plus la Cnil est informée en amont, mieux elle peut effectuer son travail de contrôle et de prévention des dommages liés aux violations de données.

Les contrôles peuvent être préalables à d'éventuelles sanctions. Le projet de loi garantit la possibilité de faire appel à des experts croisés, ce à quoi nous sommes très favorables. Nous pourrons croiser les expertises lors des contrôles menés par chaque entité : l'Anssi pourra bénéficier d'experts spécialisés dans le domaine de la protection de la vie privée et la Cnil faire appel à des experts de l'Agence.

L'échange d'informations, qui permettra d'améliorer l'efficacité des procédures, fait également l'objet de dispositions dans le projet de loi. Nous avons quelques interrogations concernant leur rédaction, notamment en ce qui concerne la notion d'« intérêts commerciaux des entités concernées ». Sans remettre en cause la nécessaire protection du secret des affaires, cette notion ne semble pas totalement bien définie. Il faudrait la supprimer ou la préciser, pour renvoyer plutôt à des « secrets protégés par la loi », afin de s'assurer que la transmission d'informations a uniquement pour objet des données nécessaires et suffisantes au contrôle et à la mise en place des procédures. Des définitions normées permettront d'éviter des problèmes *a posteriori*, en cas de contestation des procédures.

J'en viens à la coordination des sanctions. L'enjeu ne se situe effectivement pas autour du principe du *non bis in idem*, bien établi dans la jurisprudence, mais autour de l'existence d'un mécanisme qui soit complémentaire et pas surabondant. Au-delà du projet de loi, la coopération quotidienne entre les deux entités sera très importante. Il sera aussi important de prendre de manière complémentaire des mesures préalables aux sanctions, telles que des demandes de mise en conformité et des mises en demeure. Si une sanction doit être prise quand elle est nécessaire, l'objectif reste la mise en conformité. Notre collaboration avec l'Anssi est suffisamment ancienne pour que nous soyons confiants quant à notre capacité à développer une approche conjointe et non concurrentielle. Nous envisageons également de signer une convention.

Le projet de loi fait aussi référence à la stratégie nationale en matière de cybersécurité. La Cnil souhaite en être partie prenante, dans le respect de son

indépendance. Notre vision est complémentaire à celle de l'Anssi. *A contrario* de ce qui se passe pour d'autres stratégies nationales, comme celle portant sur l'intelligence artificielle, nous souhaitons jouer toute notre part dans la stratégie de l'État en matière de cybersécurité.

Ce projet de loi nous convient, même s'il peut être amélioré. L'urgence est d'en mettre en œuvre les dispositions, afin d'assurer la nécessaire montée en maturité technologique de certaines entités, notamment les PME et les collectivités. Elles seront accompagnées et auront le temps, mais il leur faut comprendre qu'elles doivent désormais se mettre en conformité. Selon une étude que nous avons récemment publiée, l'application du RGPD au domaine de la cybersécurité aura un impact économique positif pour les entreprises. Les coûts évités pourraient s'élever à plus de 100 millions grâce à une baisse de la fraude. Ce coût évité est un élément important, qui nous conduit aussi à soutenir l'adoption rapide de ce projet de loi.

M. le président Philippe Latombe. La directive NIS 2 prévoit des sanctions, notamment financières. Celles-ci se cumuleraient-elles aux sanctions liées à la non-application du RGPD ? Lors de leur audition, les responsables de l'Anssi nous ont indiqué qu'en cas de fuite des données et de problème de cybersécurité, l'amende relative au RGPD serait retenue, notamment parce qu'elle serait plus élevée.

En cas de fuite de données personnelles, la Cnil est saisie et elle garde la main si un problème de cybersécurité se pose ensuite. *A contrario*, si un problème de cybersécurité survient d'abord et qu'on se rend compte ensuite qu'il a généré une fuite de données, l'Anssi reste-t-elle responsable ou la Cnil reprend-elle la main ? Ce cas est-il déjà prévu ou faut-il l'inclure de façon plus claire dans le projet de loi ?

Au cours de nos auditions, on nous a souvent fait part de la volonté des entreprises de pouvoir accéder à une déclaration commune pour signaler des incidents auprès de l'Anssi, de la Cnil et des autorités de tutelle telles que l'Autorité des marchés financiers (AMF) ou l'Autorité de contrôle prudentiel et de résolution (ACPR) pour l'application de Dora ; qu'en pensez-vous ?

Enfin, la Cnil prend des sanctions à l'encontre des collectivités au titre du RGPD ; pouvez-vous revenir sur votre expérience en la matière ? Nombre des personnes auditionnées ont signalé une différence de traitement entre les entreprises soumises à sanction et les collectivités locales, qui ne le sont pas.

Mme Catherine Hervieu, rapporteure. Les missions de la Cnil continuent de s'étendre, en raison des décisions des législateurs européens et français, mais cette extension advient dans un contexte budgétaire contraint.

Depuis 2024, vous avez dû reporter certains remplacements d'agents et plusieurs nouveaux recrutements, qui étaient pourtant importants pour l'atteinte de vos objectifs. Dans le rapport que vous avez publié en avril 2025, il est écrit que « de nouvelles remises en cause de ses moyens financiers et humains, mettraient en risque la capacité de la Cnil à assurer de manière satisfaisante des missions pourtant

essentielles à la préservation des libertés fondamentales de chacun ». À cet égard, comment envisagez-vous l'application de ce projet de loi ?

Les collectivités sont très allantes sur le sujet du numérique, ayant compris l'importance des enjeux de gestion des données pour améliorer leur fonctionnement et des enjeux en matière de cybersécurité. Travailler avec vous représente pour elles une plus-value mais elles butent sur la question de la formation, initiale et continue des agents comme des élus, qui nécessite des moyens et des ressources humaines.

M. Michel Combot. Je comprends le besoin de simplifier les notifications d'incidents, mais le type d'informations remontées varie selon les entités ; la création d'un mécanisme unique ne serait pas neutre. Dans le cas du filtre anti-arnaque par exemple, tout le monde bute sur la question des moyens et du développement d'un système de transmission sécurisée, quand un schéma délocalisé semblerait préférable. Notre procédure est assez simple, fonctionne bien et nous évite d'avoir accès à des informations dont nous n'avons pas besoin, ce qui semble important, notamment au regard de notre objectif de minimisation des données.

Nos enjeux budgétaires ne sont pas propres au domaine de la cybersécurité. À titre d'exemple, l'entrée en vigueur prochaine du règlement sur l'intelligence artificielle posera aussi des questions de moyens.

En 2024, nous avons reçu 17 000 plaintes, dont le traitement est obligatoire au titre du RGPD. Si on les ignore, elles peuvent être contestées et les procédures peuvent remonter jusqu'au Conseil d'État voire jusqu'à la Cour de justice de l'Union européenne.

Une centaine de sanctions ont été prises, dont les deux tiers relèvent de la procédure simplifiée. Les sanctions ont une visée d'exemplarité mais doivent surtout servir à mettre en conformité et à mettre fin au préjudice, ce qui exige un traitement rapide nécessitant suffisamment de moyens.

Les collectivités doivent gagner en maturité et en compétence d'un point de vue technologique dans les domaines de la cybersécurité, de l'intelligence artificielle et de la vidéo. On sent leur volonté de bien faire, mais notre direction chargée de l'accompagnement doit avoir les moyens de mener à bien sa mission.

Les sujets que nous traitons se complexifient et représentent des enjeux forts pour nos concitoyens en matière de violations des données et de libertés. Ainsi, le sujet de l'intelligence artificielle et de la vidéo soulève des questions liées aux libertés publiques.

En ce qui concerne le développement des technologies, nous accompagnons le gouvernement sur les enjeux de protection des données et de souveraineté ; cette expertise requiert aussi des emplois. Nous avons émis nos demandes et sommes en dialogue avec les services de l'État. Il nous faut des moyens adaptés pour répondre

à la demande croissante de nos concitoyens en matière de protection et d'accompagnement, pour faire face à des enjeux qui sont au cœur du débat politique.

M. Victor Nicolle, directeur des contrôles et des sanctions de la Cnil. En ce qui concerne les moyens dévolus par la Cnil à la chaîne dite répressive, un peu plus de 50 agents se consacrent aux contrôles et aux sanctions, parmi lesquels une grosse moitié se concentrent sur les contrôles et une petite moitié sur les sanctions. En 2024, nous avons pris 88 sanctions représentant un total de 55 millions d'euros. Environ 70 sanctions relevaient de la procédure simplifiée à juge unique, qui peut donner lieu à des amendes plafonnées à 20 000 euros. Les autres sanctions relevaient de la procédure ordinaire, qui permet d'avoir recours à des amendes plus importantes.

Le principe du *non bis in idem* est inscrit au cinquième alinéa de l'article 37 du projet de loi, avec des limites. Ainsi, si les pouvoirs de la commission des sanctions de l'Anssi sont restreints, ceux de la Cnil en la matière ne le sont pas. De plus, le principe porte sur les sanctions financières qui peuvent être prononcées par l'Anssi, laissant une souplesse pour prendre d'autres mesures correctrices, telles que des mises en demeure ou des rappels aux obligations légales. Ainsi, chaque institution peut mener à bien sa mission : la continuité des activités essentielles pour l'Anssi et la protection des données pour la Cnil.

Nous reconnaissons le besoin d'articulation entre les deux entités, qui figurait dans l'avis de la Cnil du 23 mai 2024. Nous procédons déjà à des échanges substantiels concernant la chaîne répressive. Ainsi, les référentiels de l'Anssi sont utilisés de façon quotidienne par la Cnil lors de ses missions de contrôle et sont visés dans les décisions de sanction adoptées par la formation restreinte de la Cnil, au titre de normes qui s'imposent. De plus, il y a un an, la Cnil a accueilli des agents de l'Anssi pour effectuer des missions de contrôle. Des éléments de coopération existent, qui auraient vocation à être développés grâce à la coordination envisagée dans le cadre du projet de loi.

La Cnil a appelé à la création d'un mécanisme d'orientation préalable qui pourrait consister, pour l'Anssi, à informer la Cnil de façon systématique lorsqu'elle est saisie d'un incident de cybersécurité mettant en cause des violations de données et, pour la Cnil, à signaler à l'Anssi les violations dont elle aurait connaissance, notamment dans le cadre de sa chaîne répressive. Si les choses sont bien faites au stade des contrôles, l'aiguillage sera bon et les doublons seront évités en matière de sanctions.

Les dispositions de l'article 23, sous réserve de ce qu'a mentionné Michel Combot concernant la formule retenue, permettraient d'asseoir la coordination entre les deux institutions, dans le cadre d'une convention qui reste à écrire mais autour de laquelle les échanges ont débuté.

J'en viens aux collectivités territoriales. Environ 17 % des notifications de violations de données faites à la Cnil concernent des administrations publiques et la

moitié d'entre elles sont des collectivités territoriales, qui traitent des données particulièrement sensibles. L'Anssi a également relevé que ces dernières ont subi 14 % des incidents de cybersécurité qui leur ont été notifiés en 2024, soit 218.

La Cnil a déjà prononcé des sanctions à l'égard de collectivités et procède à des contrôles réguliers. Dans la perspective de la montée en régime qu'impose la transposition de la directive NIS 2, elle a fait de la cybersécurité des collectivités l'une de ses thématiques prioritaires de contrôle pour 2025. Ainsi, elle pourra contrôler les mesures organisationnelles et les mesures de sécurité interne mises en place par les collectivités pour sécuriser leurs données. Elle pourra aussi contrôler leurs sous-traitants, ce qui pourra avoir un impact important sur l'ensemble du réseau puisque certains marchés sont dévolus à seulement deux ou trois d'entre eux.

Les sanctions prononcées par la Cnil à l'encontre des collectivités territoriales tiennent compte de leurs moyens, selon les prescriptions du RGPD. Elles sont adaptées à l'objectif de mise en conformité des acteurs et peuvent prendre la forme de mises en demeure.

Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles de la Cnil. Je voudrais apporter une précision quant à l'impact des décisions de la Cnil sur les collectivités territoriales. En 2022, nous avons prononcé des mises en demeure à l'encontre de vingt-deux communes de plus de 20 000 habitants. Dans les trois mois qui ont suivi, nous avons enregistré 2 000 désignations de délégués à la protection des données, qui visaient à répondre au manquement reproché à ces communes. Ces mesures répressives ont donc un effet dissuasif et d'entraînement.

M. le président Philippe Latombe. Nous en venons aux questions des autres députés.

M. Antoine Villedieu (RN). Le projet de loi prévoit que les agents de l'État pourront accéder sans autorisation judiciaire préalable aux locaux, aux documents, aux données informatiques, voire aux informations protégées par le secret professionnel des opérateurs d'importance vitale. Ces pouvoirs, notamment inscrits aux articles R. 1332-12 et suivants du code de la défense, s'appliqueraient à des entreprises privées, à des établissements publics et même à des collectivités territoriales.

Une telle extension du pouvoir administratif sans encadrement judiciaire clair n'ouvre-t-elle pas la voie à un déséquilibre profond entre exigence de sécurité et respect des libertés fondamentales ?

Comment la Cnil évalue-t-elle ce glissement, qui pourrait faire peser une menace sur la confidentialité des échanges ou la protection des données personnelles, dans des secteurs pourtant soumis à des obligations déontologiques ou professionnelles très strictes ?

Enfin, que pensez-vous de l'introduction de garanties juridictionnelles, ne serait-ce que d'un contrôle *a posteriori*, pour éviter que la sécurité numérique ne devienne un prétexte à une surveillance administrative généralisée ?

M. Victor Nicolle. Vous évoquez les pouvoirs de l'Anssi, que nous ne sommes pas les mieux placés pour commenter.

En ce qui concerne les contrôles conduits par la Cnil, la loi « informatique et libertés » prévoit une obligation de coopération de la part des acteurs à contrôler, qu'ils soient publics ou privés. Les contrôles qui ont lieu dans les locaux des entreprises peuvent faire l'objet d'un refus, que la Cnil et les agents en charge du contrôle peuvent outrepasser en saisissant le juge des libertés et de la détention. Ce cas de figure est peu fréquent et, en général, les entreprises collaborent aux contrôles.

Quant aux secrets, ils sont encadrés par la loi « informatique et libertés ». De plus, les agents de la Cnil sont soumis à une obligation de confidentialité.

M. Michel Combot. Toutes les décisions et procédures de la Cnil sont sous le contrôle du juge administratif et peuvent être contestées, tant sur le fond que sur la forme. Ce sera sûrement le cas aussi pour les procédures de l'Anssi, qui devront répondre aux mêmes obligations en matière de déontologie et garantir que seules les informations nécessaires et suffisantes sont collectées. L'activité des entités procédant à des sanctions administratives est encadrée et une jurisprudence existe dans ce domaine. En matière de protection des libertés des individus et des entreprises, des garde-fous suffisants sont en place.

M. le président Philippe Latombe. L'existence de sanctions à l'encontre des collectivités, même si vous n'y avez pas recours, vous semble-t-elle nécessaire pour que le dispositif fonctionne ? La question nous a été posée. Le Conseil d'État répond qu'on ne peut prévoir des sanctions pour le secteur privé sans en prévoir pour la sphère publique. Selon certains, puisque les collectivités ont le désir de monter en expertise et en maturité en matière de cybersécurité, les sanctions ne sont pas nécessaires. Selon d'autres, sans sanctions les collectivités seraient moins allantes. Pensez-vous qu'il soit possible de fonctionner sans sanctions ? S'il faut en prévoir, de quel type de sanctions doit-il s'agir ? Des plans de remédiation comme vous en mettez en place sont peut-être plus efficaces que des sanctions administratives pécuniaires.

M. Michel Combot. La nature et le montant des sanctions de la Cnil sont adaptés au préjudice subi et au chiffre d'affaires de l'entité sanctionnée. Le quantum s'appliquant aux collectivités est donc forcément différent. Je le répète : nous recherchons d'abord la remise en conformité. La sanction, qui a un caractère dissuasif, tombe notamment si un acteur a bénéficié d'une situation illégale. Il est difficile de dire si les choses fonctionneraient aussi bien sans sanctions ; il s'agit d'une question éminemment politique, à laquelle il vous revient de répondre.

M. le président Philippe Latombe. Le RGPD prévoyait explicitement le cas de figure, ce qui était plus simple.

M. Victor Nicolle. Il faut entendre la sanction de façon large et ne pas se limiter à la procédure de sanction diligentée devant la formation restreinte de la Cnil. À titre d'exemple, pour des acteurs publics qu'on ne peut pas sanctionner financièrement, les mises en demeure, qui peuvent être rendues publiques, peuvent constituer une incitation très forte à se remettre en conformité. La sanction n'est pas la panacée et la sanction financière n'est pas le seul levier dont dispose la Cnil.

M. Antoine Villedieu (RN). Que pensez-vous de l'absence de garantie contre la sous-traitance hors Union européenne des services essentiels ? Je pense aux data centers, aux clouds critiques et aux réseaux.

M. Michel Combot. La question est de savoir quelles sont les données dont il s'agit et par qui elles sont détenues. Il y a un enjeu de souveraineté. Nous soutenons pleinement la stratégie du gouvernement sur le « cloud au centre », qui a été notamment transposée par la loi, visant à sécuriser et à réguler l'espace numérique, dont nous attendons des décrets d'application sur lesquels la Cnil donnera son avis.

Il s'agit d'une question politique et c'est à l'État de décider quelles sont les données soumises à un type particulier de protection. Du point de vue la Cnil, la protection de la vie privée est importante et certaines données, notamment sensibles, doivent pouvoir être écartées de l'accès extraterritorial par des pays situés hors de l'Union européenne. La définition du champ de ces données revient à l'État, notamment quand ce dernier les détient.

Pour les entreprises, dans le domaine bancaire par exemple, nous recommandons que les entreprises puissent se saisir de ce sujet important. Les solutions technologiques à appliquer ne sont pas simples ; les développer constitue un enjeu collectif, auquel la Cnil prend toute sa part.

M. le président Philippe Latombe. Le projet de loi devrait être examiné en séance au mois de septembre, ce qui nous laisse du temps. Si des sujets n'ont pas été abordés aujourd'hui, n'hésitez pas à nous faire parvenir une contribution écrite. Le but est de clarifier le plus possible le projet de loi afin de le rendre efficace et relativement accessible pour les entreprises et les administrations. Le champ de la directive NIS 2 est large et de nombreux nouveaux acteurs vont être confrontés à la mise conformité ; nous avons besoin de faire les choses le plus sereinement possible.

10. Table ronde sur la lutte contre la cybercriminalité et la cybermalveillance, mercredi 25 juin 2025 à 16 heures 30

Lors de sa réunion du mercredi 25 juin 2025, la commission spéciale a auditionné M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la cybermalveillance (GIP-ACYMA), M. Christophe Husson, général de division et chef du commandement du ministère de l'intérieur dans le cyberespace (Comcyber-MI) et Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité) du parquet de Paris.

M. le président Philippe Latombe. Nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité par l'audition de M. Jérôme Notin, directeur général du groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma) ; de M. Christophe Husson, général de division et chef du commandement du ministère de l'intérieur dans le cyberespace (Comcyber-MI) et de Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité) du parquet de Paris.

Le projet de loi que la commission spéciale est chargée d'examiner comporte trois titres. Le titre I^{er}, consacré à la résilience des activités d'importance vitale, procède à la transposition de la directive sur la résilience des entités critiques (REC) ; il est rapporté par Mme Hervieu. Le titre II vise à renforcer notre cadre juridique en matière de cybersécurité, procède à la transposition de la directive sur la sécurité des réseaux et des systèmes d'information (NIS 2) ; il est rapporté Mme Le Hénanff. Enfin, le titre III, consacré à la résilience opérationnelle numérique du secteur financier, procède à la transposition de la directive, connue sous son nom anglais, Digital Operational Resilience Ac, DORA. Il est rapporté par Mickaël Bouloux, qui s'excuse de ne pas pouvoir être présent aujourd'hui. Enfin, M. Éric Bothorel est le rapporteur général du projet de loi.

Nous avons souhaité vous entendre, car les institutions que vous représentez sont chargées à des titres très divers de lutter contre la cybercriminalité. Pourriez-vous nous dresser un état des lieux de la menace telle que vous la percevez et des moyens mis en place pour lutter contre ce phénomène inquiétant et en pleine croissance ? Je souhaiterais également recueillir votre avis sur le filtre anti-arnaque que nous avions inscrit dans la loi et qui n'est pas encore opérationnel. Quand celui-ci sera-t-il développé et mis en place ? Par ailleurs, quel est votre avis sur l'article introduit par le Sénat interdisant l'affaiblissement du chiffrement ? Dans ce contexte, nous souhaitons aussi vous entendre sur la manière dont vous percevez le projet de loi et les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du projet de loi par l'Assemblée nationale.

M. Christophe Husson, général de division et chef du commandement du ministère de l'intérieur dans le cyberespace (Comcyber-MI). Mon propos introductif a pour objet de vous présenter rapidement la manière dont le ministère de l'intérieur est organisé en matière de lutte contre la cybercriminalité, avant de

mettre en lumière l'état de la menace et quelques réflexions dans le cadre de la transposition de NIS 2, en lien avec nos différentes observations sur le terrain, notamment du côté du monde de l'entreprise.

Le Comcyber-MI est un service à compétence nationale créé le 1er décembre dernier, que j'ai l'honneur de commander. J'ai pour adjoints un policier et un magistrat. L'ensemble des autres personnels sont des militaires de la gendarmerie et des personnels civils de la gendarmerie nationale. Ce dispositif, chargé de lutter contre la cybercriminalité est organisé autour de quatre grands piliers. Le premier pilier porte sur la stratégie, puisque nous sommes en charge de définir la stratégie ministérielle de lutte contre la cybercriminalité, qui a été annoncée par le ministre délégué François-Noël Buffet le 2 avril dernier à l'occasion du Forum InCyber à Lille. Elle a vocation à être déclinée par les services de police et de gendarmerie dans des plans d'action pour chacune des entités.

Nous avons également pour mission de contribuer à porter la parole du ministère de l'intérieur sur les évolutions réglementaires et législatives, de manière à permettre aux gendarmes et aux policiers de pouvoir travailler dans les meilleures conditions possibles. Nous conduisons également une action internationale et nous sommes chargés de différentes actions de prévention et de mise à disposition des contenus au profit des forces de police et de gendarmerie pour mener des actions de prévention dans les territoires.

Le deuxième pilier concerne l'anticipation, autour de deux composantes. La première a trait au renseignement d'intérêt cyber. Nous avons pour mission de publier tous les ans un rapport sur l'état de la menace. Le premier rapport a été publié l'année passée, au mois de juillet, et le rapport 2025 le sera dans les jours à venir. Au-delà, nous réalisons des fiches d'alerte flash sur différents phénomènes, que nous diffusons de manière très large, à la fois au sein du ministère, auprès des autres administrations, et de l'écosystème privé. À titre d'exemple, cette division de l'anticipation est d'ailleurs présente au sein du Campus Cyber, de manière à être connectée à l'écosystème privé, au monde de la recherche et au monde universitaire. Dans l'anticipation, nous menons également des actions en matière de gestion de crises, en particulier sur des sujets qui sont liés à la prévention.

Nous n'intervenons pas directement sur l'accompagnement à la gestion de crises, mais plutôt à la préparation, notamment des entreprises ou des collectivités. À ce titre, nous avons réalisé en collaboration avec cybermalveillance.gouv.fr un module de formation en ligne (Mooc) d'une durée d'à peu près deux heures, qui permet de se poser les bonnes questions sur une crise potentiellement naissante. Ce Mooc est régulièrement utilisé par des entreprises, dans le cadre de l'accompagnement et de la préparation à une gestion de crise cyber.

Le troisième pilier porte sur la formation. Notre centre national de formation continue de haut niveau en matière cyber est situé à Lille. Il forme des policiers et des gendarmes de la France entière, par exemple sur le blanchiment des cryptomonnaies ou encore l'enquête sous pseudonyme. Nous avons aussi élargi les

formations au *continuum* de sécurité à différents acteurs en charge de la lutte contre la cybercriminalité tels que des magistrats, mais aussi quelques entités du ministère de l'économie et des finances.

Enfin, le quatrième pilier est d'ordre pilier opérationnel, c'est-à-dire apporter un appui aux services de police et de gendarmerie spécialisés dans le cadre des enquêtes judiciaires sur des compétences dites rares. Je pense en particulier au blanchiment des cryptomonnaies, sujet majeur aujourd'hui et largement utilisé dans le cadre de la criminalité organisée, mais aussi au traitement de la donnée de masse ou l'expertise numérique du haut du spectre sur tous les objets connectés.

Les différentes directions du ministère disposent, à leur niveau, d'un service spécialisé en matière d'enquête judiciaire. Pour la police nationale, il s'agit de l'Office anti-cybercriminalité (Ofac), qui est en charge de la coordination opérationnelle des services ; l'Unité nationale cyber (UNC) pour la gendarmerie et la Brigade de lutte contre la cybercriminalité (BL2C), sans parler de la direction générale de la sécurité intérieure (DGSI) dans un domaine de compétences très particulier.

S'agissant de l'état de la menace, notre prochain rapport sera publié dans quelques jours. Il portera à la fois sur les atteintes fortes aux biens et les atteintes aux personnes. Les atteintes aux biens, qui représentent globalement deux tiers des infractions enregistrées, correspondent, pour 80 % d'entre elles, à des escroqueries sur internet. Les 20 % restants portent sur des atteintes au système de traitement automatisé des données, notamment les attaques par rançongiciel, sans doute les plus dévastatrices sur les systèmes d'information. Ce phénomène important touche typiquement les territoires, en métropole ou en outre-mer, les collectivités territoriales de toute taille, les petites et moyennes entreprises (PME), les entreprises de taille intermédiaire (ETI), les hôpitaux, les professions de santé en général. Il y a quelques années, les grands groupes industriels étaient les principales victimes. L'adversaire s'est largement adapté et aujourd'hui, il part à la chasse sur tous les types de structures ; tout le monde peut être concerné. En conséquence, la mise à niveau de la maturité cyber dans les territoires pour les différentes entités est importante pour la résilience globale de notre système économique.

S'agissant des atteintes aux personnes, nous observons un certain nombre de sujets liés à la pédopornographie, au cyberharcèlement, sur les réseaux sociaux notamment, et internet en général.

Ensuite, je souhaite offrir un éclairage sur la partie prévention. Le Comcyber-MI est notamment en charge de transmettre aux services de police et de gendarmerie des éléments de langage pour mener la prévention dans le territoire. Je tiens à évoquer à ce titre une action historiquement conduite par la gendarmerie nationale, c'est-à-dire une action de diagnostic cyber, notamment au profit des collectivités territoriales, mais qui a ensuite été déclinée au profit des entreprises.

Elle a débuté en 2021 avec un questionnaire d'autodiagnostic de dix questions qui a démontré que les risques étaient plutôt de nature « rouge » que « verte », ce qui était assez problématique. La gendarmerie a souhaité aller plus loin, en développant un pré-diagnostic de 70 à 120 questions en fonction de la taille de la collectivité. Ce questionnaire comporte surtout des questions « de bon sens » posées à l'entité en charge de la collectivité, au-delà des directeurs des systèmes d'information (DSI). Il a permis de révéler que de nombreuses collectivités n'étaient pas au niveau de maturité cyber que l'on aurait pu espérer.

Dans cette action, nous avons souhaité nous rapprocher de l'Agence nationale de la sécurité des systèmes d'information (Anssi), à la suite de la création du Comcyber-MI. L'Anssi a ainsi développé l'outil MonAideCyber, vers lequel le ministère de l'intérieur s'oriente en matière de diagnostic. MonAideCyber figure aujourd'hui dans la stratégie ministérielle de lutte contre la cybercriminalité. Après les collectivités, nous nous sommes tournés vers les entreprises pour pouvoir assurer un certain nombre de diagnostics. Les différents outils disponibles (autodiagnostic, pré-diagnostic et audit) ne disposent pas tous de la même profondeur de champ, ce qui pose la question de savoir lesquels utiliser, selon quels besoins.

Ensuite, que faire ? Dès lors que le constat d'une maturité cyber insuffisante pour une collectivité ou pour une entreprise est posé, les services de police ou de gendarmerie n'orientent pas vers un prestataire de services mais vers cybermalveilliance.gouv.fr qui dispose dans les territoires d'une liste d'entités référencées ou labellisées, ou vers les CSIRT régionaux, qui disposent d'entités référencées. Dans ce cadre, l'enjeu de la coordination est essentiel, les entreprises ou les collectivités évoquant souvent les sujets de visibilité, ce qui soulève la question de la labellisation.

Le Comcyber-MI noue également des liens très étroits avec l'Anssi, incontournable sur NIS 2. Nous avons besoin que nos gendarmes et nos policiers disposent d'une bonne connaissance des éléments essentiels de NIS 2, afin qu'ils puissent communiquer et répondre aux questions. Nous élaborons actuellement avec l'Anssi un document simple à cet effet, mais également un document plus élaboré pour les personnels qui effectueront des diagnostics dans le cadre de MonAideCyber.

Par ailleurs, les forces de sécurité intérieure ont besoin d'être alertées dès lors qu'une attaque cyber est connue. Au-delà de la priorité principale d'une entreprise ou d'une collectivité qui cherchent à rétablir un système d'information, il nous faut récupérer des éléments techniques nous permettant de localiser, voire d'identifier un auteur. Nous avons donc besoin d'une coordination entre la victime, le cas échéant l'Anssi, les entités de remédiation et les services enquêteurs. Il s'agit là du principe du « Dites-le-nous une fois ».

S'agissant du filtre anti-arnaque, je préfère laisser Jérôme Notin évoquer le sujet, le Comcyber-MI n'étant pas directement impacté. Vous avez également mentionné l'affaiblissement du chiffrement. Plutôt que de répondre sur

l'affaiblissement du chiffrement en tant que tel, je préfère évoquer la question du besoin des enquêteurs. La plupart des enquêtes judiciaires concernent une multitude de données, raison pour laquelle le Comcyber-MI dispose d'une compétence rare, le traitement de la donnée de masse.

Dès lors que la donnée est chiffrée, nous ne pouvons pas y accéder, ce qui affecte la recherche d'éléments permettant d'établir la manifestation de la vérité. Les messageries chiffrées EncroChat, Sky ECC ou plus récemment Ghost ou Matrix sont des dispositifs mis en place par des réseaux criminels, mais nous avons pu accéder aux données, ce qui nous a permis de démanteler un certain nombre de réseaux de criminalité organisée et conduire des interpellations à travers le monde. En résumé, les enquêteurs ont besoin de pouvoir accéder à la donnée.

Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité) du parquet de Paris. La section J3 dédiée à la lutte contre la cybercriminalité du parquet de Paris dispose d'une compétence nationale concurrente, c'est-à-dire qu'elle a vocation à se saisir des affaires du haut du spectre, les dossiers qui ont un intérêt pour la sécurité de la nation et qui impliquent de disposer d'une centralisation de l'information et de l'enquête. Le reste des dossiers sera quant à lui laissé aux parquets locaux. Naturellement, il existe un magistrat référent cyber dans chaque parquet de France, avec lequel il est possible de dialoguer, d'échanger.

La section J3 est une petite section composée de cinq magistrats ; de deux assistants spécialisés, c'est-à-dire du personnel spécialement formé techniquement pour nous aider ; une attachée de justice dédiée à la lutte contre la cybercriminalité qui apporte un soutien du point de vue de la coopération internationale ; et d'une équipe de greffiers. Cette section a crû au fil des années, à mesure que la menace s'est développée.

Le rôle de la justice consiste à traduire les cybercriminels devant des juridictions, afin qu'ils soient jugés et condamnés pour les infractions qu'ils ont commises. Lorsque ces auteurs sont situés dans des pays qui ne coopèrent pas, qui n'exécutent pas les demandes d'extradition, l'intérêt de l'enquête consiste à pouvoir émettre des mandats d'arrêt, ce qui signifie que les cybercriminels ne pourront plus quitter le pays. Même s'il n'y a pas de condamnation, cette menace du mandat d'arrêt est extrêmement forte et puissante.

Au-delà des questions d'arrestation et de jugement, qui constituent véritablement le cœur de notre métier, nous luttons ces dernières années contre les infrastructures criminelles. Ce faisant, en démantelant des réseaux de *botnets* derrière les attaques, nous empêchons les criminels de pouvoir attaquer nos institutions, nos entreprises. De même, nous saisissons des avoirs criminels, comme des *wallets* de cryptomonnaies riches de plusieurs dizaines de millions d'euros, affaiblissant ainsi les réseaux. Cet argent saisi permet d'indemniser les victimes, et lorsque celles-ci ne peuvent être identifiées, il est reversé à l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (Agrasc), l'agence chargée de gérer

les avoirs criminels pour la justice. Elle pourra ensuite l'utiliser pour mener d'autres actions, permettre aux magistrats et aux enquêteurs d'être plus efficaces.

Une autre action, plus novatrice, consiste à utiliser le canal judiciaire comme un canal diplomatique. Dans certains cas, notamment pendant les Jeux olympiques, nous avons pu identifier que des pays nous avaient attaqués, probablement à travers leurs services. Nous leur avons donc envoyé une demande d'entraide, par exemple pour identifier le titulaire de l'adresse IP utilisée. Nous savions parfaitement que nous n'obtiendrions pas de réponse, mais à travers le canal judiciaire, nous leur avons fait savoir que nous avions connaissance du fait qu'ils étaient responsables de l'attaque.

Les différents moyens mis en œuvre par la section cyber contribuent à la lutte contre la cybercriminalité de façon générale. De façon indirecte, nous parvenons aussi à capter des renseignements. Grâce à l'article 706-105-1 du code de procédure pénale, nous avons la possibilité de communiquer l'information judiciaire de nos dossiers cyber aux différents services de l'État : l'Anssi, la DGSI, la direction générale de la sécurité extérieure (DGSE), le Comcyber des armées. Ces éléments leur permettent d'avoir une meilleure compréhension de la menace, d'assembler les pièces du puzzle, et de pouvoir mener une riposte. De fait, la justice et l'action du parquet contribuent, avec celles des autres services de l'État, à une riposte globale de la France.

À présent, je souhaite vous dresser un rapide panorama de la menace. Comme le général Husson l'a signalé, la première menace concerne les rançongiciels, car ils frappent le tissu économique, déstabilisent nos hôpitaux, nos collectivités locales. Ces rançongiciels se sont perfectionnés et nous sommes aujourd'hui confrontés à des groupes extrêmement structurés, dotés d'une véritable organisation criminelle. Pour autant, nous parvenons à obtenir des résultats. Je pense par exemple au dossier LockBit ou à l'auteur du rançongiciel Ako que nous avons jugé le mois dernier au tribunal judiciaire de Paris.

Néanmoins, je dois vous faire part d'un constat plus préoccupant, qui concerne la transformation numérique de la délinquance. Lorsque j'ai commencé à la section de lutte contre la cybercriminalité en 2017, nous nous concentrions surtout sur les piratages en tant que tels. Aujourd'hui, nous nous apercevons que les groupes criminels, qui n'étaient pas présents dans le cyber initialement, se sont « numérisés ». Dans la mesure où la société est complètement digitalisée, les surfaces d'attaque ont augmenté.

À titre d'exemple, auparavant, les narcotrafiquants ne pratiquaient pas le piratage informatique. Aujourd'hui, ils piratent les logiciels dans les ports pour faire passer des conteneurs de cocaïne, s'adjoignent les services de hackers pour pouvoir être plus discrets dans la communication. Nous assistons à une transformation générale de cette délinquance. Dans certains de nos dossiers, des groupes de délinquance habituels ont recruté des ingénieurs informatiques pour des sommes extravagantes, parfois 1 million d'euros.

Il faut retenir que maintenant, tous les groupes criminels ont un intérêt à attaquer un système de traitement automatisé de données, qu'ils ne travaillent pas en silos, mais que les narcotrafiquants et les hackers voient leur intérêt à unir leurs forces. À ce titre, il convient de mentionner le dossier « Dark Bank », une banque occulte mise à jour grâce au dossier Sky ECC. Cette banque a blanchi l'argent des narcotrafiquants, c'est-à-dire du cash, soit 1 milliard de dollars en dix-huit mois. Les hackers avaient beaucoup de cryptomonnaies et voulaient du cash, quand les narcotrafiquants avaient la problématique inverse. En conséquence, cette banque a fait chambre de compensation entre ces deux univers.

Ces deux éléments doivent être gardés à l'esprit aujourd'hui lorsque l'on parle de résilience. Nous serons de plus en plus attaqués parce que nous sommes de plus en plus digitalisés, parce que les groupes criminels traditionnels auront besoin de s'attaquer à ces vecteurs pour commettre des infractions, par exemple de narcotrafic. Le constat n'est guère réjouissant : les organisations criminelles ont intégré la digitalisation et le vecteur numérique comme une composante à part entière de leur activité. Face à cette menace grandissante, nous devons être plus efficaces dans notre réponse, encore progresser d'un cran.

S'agissant des questions plus spécifiques de M. le Président, je laisserai Jérôme Notin évoquer le filtre anti-arnaque, sujet sur lequel il est très engagé. Ensuite, lors des débats sur l'affaiblissement du chiffrement dans le cadre de la loi de lutte contre le narcotrafic, le parquet de Paris a été sollicité pour prendre position. Nous ne l'avons pas fait, pour différentes raisons, notamment parce que nous estimions que cette question ne relevait pas de notre compétence.

Néanmoins, à mon niveau, je peux vous fournir quelques éléments d'analyse. Nous avons évidemment besoin de pouvoir déchiffrer de la donnée pour nos enquêtes. À ce titre, le véritable enjeu consiste à savoir si l'on peut déchiffrer cette donnée sans affaiblir le chiffrement. Le service technique national de captation judiciaire (STNCJ), qui dépend de la DGSI, est censé effectuer des captations, c'est-à-dire hacker les téléphones, les serveurs et les ordinateurs, pour récupérer la donnée au profit de la police, de la gendarmerie et, *in fine*, de la justice. Ce service, qui a mis du temps à éclore, a obtenu des résultats assez prometteurs ces dernières années. Il doit continuer à pouvoir disposer de capacités pour pouvoir progresser.

Mais, au-delà, j'ai déjà proposé la création d'une véritable direction technique, qui serait co-dirigée par les deux ministères de la justice et de l'intérieur. À ce titre, le SNCJ pourrait intégrer cette agence, au même titre que l'Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ), qui est chargée des interceptions téléphoniques pour la justice, pour venir au soutien de nos enquêtes.

La question ne consiste pas à savoir s'il faut affaiblir le chiffrement, mais quels moyens techniques la justice, la police et la gendarmerie ont à leur disposition pour mener des enquêtes. En créant cette véritable direction technique, qui existe à la DGSI et à la DGSE, vous armeriez la justice pour répondre à ces enjeux. À titre

d'exemple, notre section cyber est souvent sollicitée par des collègues magistrats, qui souhaitent notre éclairage sur les possibilités techniques dans des dossiers de droit commun. Si cette agence était créée et dotée de véritables moyens humains, techniques et financiers, elle pourrait accomplir ce travail au profit de toutes les juridictions.

M. Jérôme Notin, directeur général du groupement d'intérêt public Acyma. Je commencerai mes propos par une présentation succincte de notre dispositif, la manière dont nous percevons le projet de loi et dont nous pensons que nous pourrions être impliqués, avant d'aborder filtre anti-arnaque ainsi qu'un petit point d'actualité sur le chiffrement. Je précise également que la proposition de Mme Johanna Brousse concernant la création d'une direction technique co-dirigée par la justice et l'intérieur me paraît tout à fait opportune.

S'agissant de l'état de la menace, nous publions un rapport d'activité tous les ans, puisqu'en tant que dispositif national d'assistance aux victimes d'actes de cyberviolence, nous sommes au contact direct des victimes, particuliers, entreprises et collectivités. L'année dernière, la plateforme cyber-malveillance.gouv.fr a accueilli 5,4 millions d'utilisateurs, contre 3,7 millions en 2023. Sur cette plateforme, nous offrons des parcours de qualification de la menace, en fonction des différents profils, pour proposer aux victimes des conseils adaptés, une mise en relation avec des prestataires. Nous avons ainsi cartographié sur l'ensemble du territoire des prestataires référencés et des prestataires labellisés.

Depuis le 17 décembre dernier, il existe une mise en relation avec un policier, un gendarme, vingt-quatre heures sur vingt-quatre, sept jours sur sept, à travers le 17Cyber. Nous sommes passés de 280 000 parcours d'assistance toutes victimes confondues en 2023 à 420 000 parcours, soit une multiplication par deux depuis la mise en place du 17Cyber.

Les assujettis à NIS 2 sont du ressort de l'Anssi. En revanche, compte tenu du travail que nous avons effectué depuis de nombreuses années, nous pensons pouvoir intervenir à deux niveaux. Le premier niveau concerne la prévention et la sensibilisation. La directive fait à de nombreuses reprises référence à la nécessité d'actions de prévention. L'article 5 *bis* ajouté par le Sénat évoque la stratégie nationale et dans un de ses alinéas, il précise que des campagnes massives doivent être réalisées pour les différents assujettis. L'année dernière, le texte de la Commission supérieure du numérique et des postes (CSNP) sur NIS 2 recommandait aussi des actions de prévention.

Je propose ainsi qu'à l'article 5, nous puissions être identifiés comme le dispositif qui porte ces actions de prévention, en lien avec la stratégie nationale pour les années 2025-2030. Lors de vos auditions a souvent été évoqué le fait que la sensibilisation ne fonctionnait pas toujours ; mais ceci est dû à l'insuffisance de moyens dont nous disposons pour conduire des campagnes de sensibilisation sur le modèle de la sécurité routière, qui dispose d'un budget de 20 millions d'euros pour effectuer ses campagnes, depuis des dizaines d'années.

Ensuite, les prestataires labellisés constituent un début de réponse à une partie des problèmes sur la partie relative à la sécurisation et l'accompagnement des collectivités, des très petites, petites et moyennes entreprises (TPE-PME) dans les territoires qui seront assujettis à NIS 2. L'Anssi, qui est membre de notre comité de pilotage du label, a compris le rôle de nos prestataires experts cyber. Dans le cadre de groupes de travail avec l'Anssi, nous avons évalué le niveau de notre référentiel de labellisation et des référentiels techniques.

Le GIP est convaincu que grâce à une petite formation et avec l'aide complémentaire d'une structure qui pourrait être l'autorité nationale, nous serons en mesure d'identifier les prestataires. Pour le dire très simplement, il nous manque aujourd'hui des leviers pour fidéliser ces prestataires et nous sommes convaincus que NIS 2 constituerait une bonne opportunité pour leur permettre d'accompagner la sécurisation des structures qui en ont besoin, mais ne savent pas vers qui se tourner quand elles identifient cette problématique.

La directive précise par ailleurs que « *Les États membres peuvent mettre en place au niveau national un mécanisme de financement destiné à couvrir les dépenses nécessaires à l'exécution des tâches des entités publiques chargées de la cybersécurité dans l'État membre en vertu de la présente directive* ». La CSNP recommandait déjà en octobre dernier d'allouer des crédits supplémentaires au secrétariat général de la défense et de la sécurité nationale (SGDSN) dans le cadre du programme 129 pour le projet de loi de finances (PLF) pour 2025, fléchés vers le GIP Acyma.

De fait, il y a urgence ; le budget 2025 du GIP a baissé de 120 000 euros par rapport à 2024 et il continuera à diminuer l'année prochaine puisque l'un de nos nouveaux membres nous quitte. Or chaque année, je ne dispose que 200 000 à 300 000 euros pour engager des actions de prévention et de communication. De plus, deux personnes qui étaient mises à disposition par nos membres sont reprises par leur structure d'origine. En outre, le dernier rapport de la Cour des comptes sur NIS 2 souligne la problématique de lisibilité, mais le 17Cyber, en tant que guichet unique, devrait précisément apporter une réponse à cette problématique. J'estime que nous ne coûtons pas beaucoup d'argent à l'État français, mais que les impacts que nous pouvons engendrer sont quand même assez importants.

Ces contraintes budgétaires nous ont de fait conduits à stopper la campagne de prévention que nous menions avec l'Institut national de la consommation (INC) sous le format des Conso Mag, qui nous permettaient de toucher des millions de téléspectateurs. De la même manière, nous avons été contraints de refuser de travailler avec le Comcyber-MI sur la version 2 de SenCy-Crise, alors que nous étions très heureux de contribuer à la première mouture. Je n'étais pas en mesure d'allouer une somme qui vous paraîtra dérisoire, 20 000 à 30 000 euros, nécessaire à l'évolution de notre plateforme pour l'hébergement de la nouvelle version.

S'agissant du filtre anti-arnaque, j'ai eu l'occasion de dresser un historique puisque nous avions rendez-vous la semaine dernière avec le cabinet de Clara

Chappaz. En septembre 2022 s'est déroulée une première réunion de lancement, portée par le ministère du numérique, qui a confié à notre GIP le soin d'étudier la mise en place du filtre anti-arnaque. En trois mois, nous avons produit un rapport, qui s'inspirait notamment du modèle belge, extrêmement pragmatique et qui fonctionne. Ce rapport a été remis au ministre Jean-Noël Barrot en janvier 2023. Nous indiquions à cette occasion que le délai de développement serait d'une dizaine de mois à partir du moment où nous recevrions les financements.

Le ministre a pris l'engagement d'un démonstrateur pour la Coupe du monde de rugby à l'automne 2023, puis d'un filtre opérationnel pour les Jeux olympiques. Mais plusieurs mois se sont passés sans nouvelle du ministère. Ensuite, pendant une longue période, nous avons été confrontés à un problème avec la direction générale des entreprises (DGE) à Bercy sur la qualification juridique de la convention nous concernant, ces services nous orientant vers une convention de mandat, laquelle ne nous permet pas de sous-traiter. Or nous devions construire et héberger un *data center* dans un SecNumCloud. Finalement, la DGE a décidé de passer un marché de gré à gré de 10,8 millions d'euros en février 2024, auquel nous avons répondu initialement par une offre à 7,2 millions d'euros, en l'assortissant de réserves par rapport à certaines exigences de sécurité.

La DGE nous a ensuite indiqué qu'elle ne disposait que de 5,9 millions d'euros. Nous avons aligné notre offre sur ce montant, mais en réduisant nécessairement le périmètre du maintien en condition opérationnelle et de sécurité, de 36 mois à 30 mois. En juillet 2024, la DGE nous a notifié que la procédure était déclarée sans suite pour un « motif d'intérêt général » tenant à l'insuffisance des ressources financières de la direction bénéficiaire, c'est-à-dire elle-même.

En janvier 2025, la direction interministérielle du numérique (Dinum) a été mandatée pour établir une contre-proposition à notre proposition et nous a contactés. Nous nous sommes rencontrés, avant de tenir une réunion en mars avec la dizaine d'autorités administratives impliquées dans la mise en place ou l'exploitation du filtre. Finalement, vendredi dernier, au cabinet de Clara Chappaz, nous avons échangé d'une manière très constructive avec la Dinum.

De son côté, la DGE nous a annoncé qu'elle ne voulait pas mettre en place le filtre, mais nous nous en doutions déjà, puisque cette administration remet en cause les choix de son ministre, voire du président de la République, dès lors que le filtre anti-arnaque était un engagement du président pour sa réélection. Cela ne peut que poser question. Finalement, la ministre arbitrera entre, *a priori*, la Dinum et Acyma pour décider de la structure qui développera et opérera le filtre anti-arnaque.

M. Éric Bothorel, rapporteur général. Vous êtes les grands témoins de la nécessité de ce projet de loi. À ce stade, je tiens, à travers vous, à remercier les équipes qui œuvrent chaque jour, au quotidien et dans vos domaines respectifs, à la lutte contre la cybercriminalité. Vous êtes au cœur de la stratégie nationale de cybersécurité qui vient d'être validée. Je centrerai mon intervention et mes

questions sur les propositions et préconisations qui vous concernent dans cette stratégie et qui pourraient être intégrées à ce projet de loi.

Madame Brousse, face à l'escalade des cybermenaces et à cette sophistication croissante des cybercrimes, le renforcement des capacités judiciaires françaises en matière de lutte contre la cybercriminalité constitue une nécessité impérieuse. L'enjeu crucial pour la France est double : améliorer l'efficacité des investigations judiciaires pour identifier et traduire en justice les cybercriminels et renforcer ces capacités à décourager toute forme de cybercriminalité en envoyant le message que la cybercriminalité ne sera pas impunie.

Les capacités d'investigation spécialisée des services compétents seront renforcées. Cela implique d'une part de doter le parquet spécialisé de Paris, compétent au niveau national, de ressources nécessaires pour mener des enquêtes complexes et aboutir à des condamnations. Je n'évoquerai pas la compétition qui pourrait exister entre le parquet national anticriminalité organisée (Pnaco) récemment créé et le J3, dont l'excellence et l'expertise sont reconnues de tous. Vous avez clairement souligné que les criminels ne s'exonèrent pas de mettre en œuvre des moyens cyber. Disposez-vous des moyens à la hauteur des ambitions en matière de cybercriminalité ? En outre, vous avez évoqué l'existence de magistrats référents cyber dans chaque parquet. Ce dispositif fonctionne-t-il ? Faut-il poursuivre son développement ?

Par ailleurs, le cadre légal judiciaire, en particulier le code de procédure pénale, devra également évoluer pour tenir compte des spécificités de la cybercriminalité. Parmi les adaptations nécessaires, différents éléments sont cités. Il s'agirait d'abord de la création d'un cadre pour conduire les opérations de démantèlement et de désinfection à distance des supports informatiques utilisés par des systèmes criminels à l'insu de leurs propriétaires légitimes, afin de faire cesser l'infraction. Il s'agirait ensuite de la création d'une infraction spécifique de fraude informatique. Cette infraction permettrait de sanctionner plus efficacement les actes de piratage informatique, d'intrusion dans les systèmes informatiques et de vol de données.

Il est également question de la modification de l'infraction de plateformes en ligne. Cette infraction actuellement limitée à la diffusion de contenus illicites, devrait être élargie pour couvrir d'autres types d'infractions commises sur les plateformes en ligne, comme la cybercriminalité. Quel est votre point de vue sur ces évolutions du code de procédure pénale ?

Enfin, un débat a lieu concernant la fragilité du cadre juridique actuel sur la pratique du renseignement d'origine sources ouvertes (Osint), notamment pour des institutionnels comme vous. Est-il nécessaire de renforcer notre cadre légal pour la pratique de l'Osint, en établissant par exemple que certains acteurs soient plus légitimes que d'autres à le pratiquer ?

Mme Johanna Brousse. S'agissant des moyens alloués à la justice, nous espérons effectivement un renforcement des capacités de J3, à la fois en termes d'assistants spécialisés, d'attachés de justice, et de magistrats. Un sixième magistrat doit nous rejoindre en septembre ; nous espérons que cela sera effectif. Il est certain qu'il faut continuer à monter en puissance si nous voulons pouvoir nous donner les moyens de répondre à cette menace.

Il convient d'être extrêmement vigilant concernant le périmètre de la section de lutte contre la cybercriminalité. Nous défendons l'idée qu'une section cyber ait la primauté sur le Pnaco ou sur d'autres juridictions sur ce qui doit être centralisé ou non au niveau national. En effet, il ne faut pas que la centralisation de l'information s'effrite. La section cyber doit pouvoir continuer à disposer en priorité de ce droit de se saisir des dossiers cyber. La centralisation de l'information nous permet de créer des liens, de collecter des éléments et d'être efficaces.

S'agissant des nouvelles infractions suggérées, il est évident que notre arsenal législatif devra se renforcer pour pouvoir s'adapter aux nouvelles techniques émergentes. Aujourd'hui, plusieurs dossiers ont été classés ou ont même fait l'objet de relaxe, en raison d'un vide juridique.

Laissez-moi l'illustrer par un exemple très concret. Certains individus ont profité d'une vulnérabilité sur un site et ont rempli leur compte de cryptomonnaies simplement en cliquant. Ils sont devenus millionnaires. Ils ne pouvaient pas être poursuivis pour vol parce qu'il ne s'agissait pas d'une soustraction frauduleuse. Le ministère de la justice nous a incités à les poursuivre pour escroquerie, mais il n'y a pas eu de manœuvre frauduleuse. Ils ont donc obtenu une relaxe en première instance, puis en appel.

Face à ce vide juridique, il serait sans doute opportun de réfléchir à la création d'une nouvelle infraction, la fraude informatique. Elle existe déjà dans d'autres pays et permettrait d'étoffer utilement l'arsenal législatif français. Le délit d'administration de plateforme a été créé en 2023 dans la loi d'orientation et de programmation du ministère de l'intérieur (Lopmi) et nous a par exemple permis de faire fermer la plateforme Coco.gg. Le potentiel de cette infraction pourrait effectivement être renforcé si le texte était écrit de manière plus englobante, ce qui nous permettrait également de lutter plus efficacement contre les ingérences numériques étrangères.

De très grands efforts ont déjà été accomplis sur ce sujet, notamment avec la proposition de loi de Sacha Houlié sur la création d'une circonstance aggravante d'ingérence étrangère, mais il est possible d'aller encore plus loin. Plus globalement, il faudra réfléchir à certaines techniques spéciales d'enquête. Nous nous appuyons un texte générique, sur la perquisition et la captation pour les mettre en œuvre, mais nous ne sommes pas certains que les techniques utilisées rentrent dans ce cadre.

S'agissant de l'Osint, concrètement, nous utilisons ce que nous trouvons en sources ouvertes sur internet pour documenter nos procédures. Des propositions émergent en la matière, dans la mesure où des acteurs privés, mais aussi des enquêteurs peuvent se sentir en insécurité dans l'utilisation des *leaks*. Pour notre part, nous considérons que nous pouvons les employer en procédure. Peut-être faut-il en passer par un texte de loi pour clarifier la situation et rassurer l'ensemble de l'écosystème cyber. Mais la question se pose également en termes de compétitivité française. Certaines grandes entreprises m'indiquent ainsi qu'elles préfèrent acheter des solutions étrangères, qui ne se posent pas la question de savoir si les données ont été piratées ou non. Les entreprises françaises essayent de jouer le jeu, mais elles ne savent pas si elles ont le droit de récupérer les *leaks*. En conséquence, elles hésitent à agir de la sorte et me posent la question. Je leur réponds que je pratique de cette manière dans mes enquêtes, mais que je n'ai pas aujourd'hui l'autorisation de leur dire si elles ont la capacité de le faire, car cela peut correspondre à du recel de délit.

M. Christophe Husson. Ce point fait l'objet de nombreuses réflexions du ministère de l'intérieur, dans le cadre de l'entité CIRSO-MI, le centre des investigations et des recherches en source ouverte du ministère de l'intérieur. Elle rassemble l'ensemble des services de police et de gendarmerie, mais également les services de renseignement. Ces entités s'interrogent en effet sur les *leaks* qui seraient utilisés dans le cadre de l'enquête judiciaire ou du renseignement. Le ministère de l'intérieur a réfléchi à un texte qui pourrait être proposé dans ce cadre, mais uniquement sur son propre périmètre du ministère de l'intérieur.

Mme Anne Le Hénanff, rapporteure. Je vous ai écouté attentivement. Je rappelle en préambule qu'il ne s'agit pas non plus de surtransposer la directive. Ensuite, à la lumière des constats que vous dressez, j'observe que les moyens qui seront accordés seront essentiels dans la transposition de NIS 2, qu'il s'agisse des moyens financiers ou des moyens humains. Je déplore par ailleurs que 80 % des décrets d'application de la loi visant à sécuriser et à réguler l'espace numérique (Sren) que nous avons voté il y a peu, n'aient toujours pas été publiés.

Monsieur Notin, comment envisagez-vous l'impact direct, opérationnel sur vos sollicitations lorsque la loi de transposition de NIS 2 sera promulguée ? En avez-vous estimé le nombre ? Disposez-vous de suffisamment de moyens pour y répondre ? Visiblement, cela ne semble pas être le cas.

Je souhaite également évoquer les collectivités territoriales. L'Anssi a proposé un seuil de 30 000 habitants dans le cadre de NIS 2. Quel est votre avis à ce sujet ? Dans certains cas de figure, il apparaît pertinent, parce qu'il faut bien établir une limite, mais dans d'autres, il semble que cela n'ait pas de sens. Certaines communes n'ont pas de DSI, et encore moins de responsable de la sécurité des systèmes d'information (RSSI). Les systèmes d'information sont interconnectés avec ceux de l'intercommunalité. Certaines communes détiennent des compétences en matière d'eau, essentielles pour NIS 2, mais comportent moins de 10 000 habitants. J'aimerais connaître votre point de vue à ce sujet, ainsi que sur la chaîne

des sous-traitants, dans la mesure où NIS 2 sera diffusée bien au-delà des 15 000 entités ciblées.

Madame Brousse, je vous remercie pour votre présentation. J'aimerais que vous puissiez également nous donner votre avis sur le hacker « éthique » qui, s'il n'est pas évoqué noir sur blanc dans le texte, figure en toile de fond. Cette notion a-t-elle un sens ? Je rappelle ainsi que le considérant 60 de la directive NIS 2 indique que les États membres doivent protéger les hackers éthiques sans les citer nommément. Que pensez-vous du cadre juridique existant en la matière ? Devrons-nous l'approfondir ?

Enfin, vous avez souligné que la voie judiciaire devient parfois une voie diplomatique, lorsque vous transmettez une adresse IP à un État étranger. En quoi est-ce efficace, concrètement ? Cela contribue-t-il à faire cesser les attaques ?

Mme Sabine Thillaye (Dem). La Cour des comptes a évoqué la confusion des écosystèmes cyber, la multiplicité des acteurs étatiques impliqués sans qu'il n'existe pour autant de véritable gouvernance unifiée. Pensez-vous qu'une telle gouvernance est souhaitable ?

Ensuite, nous comprenons bien que les financements sont le nerf de la guerre. Que se passera-t-il si ceux-ci ne peuvent être obtenus ? Par ailleurs, en tant que parlementaires, comment pouvons-nous mieux sensibiliser dans nos circonscriptions, dont certaines sont très rurales ?

Mme Laetitia Saint-Paul (HOR). Général, je m'interroge sur les enjeux de vidéosurveillance et de reconnaissance faciale. Dans quelles mesures les freins juridiques existant actuellement sur l'utilisation de ces moyens affectent notre efficacité pour arrêter les criminels ? Vous avez parlé du blanchiment des cryptomonnaies. Pourriez-vous détailler de quelle manière ce blanchiment rejaillit dans l'économie réelle ? J'ajoute qu'un rapport sénatorial traite de la place de l'or dans le blanchiment d'argent. Par ailleurs, pourriez-vous nous faire parvenir votre rapport sur l'état de la menace quand il sera publié ? S'agissant du partage de l'information, vous étiez plutôt rassurants, mais n'existe-t-il pas un émiettement des acteurs ? Ce partage fonctionne-t-il bien avec les armées, la DGSI, le SGDSN ?

Madame la procureure, je m'intéresse aux liens entre criminalité étatique et non étatique. Avez-vous des exemples à nous soumettre à ce titre ? Je souhaiterais également en savoir plus sur les liens entre les différentes criminalités, les enjeux de radicalisation en matière de terrorisme. Les mêmes outils sont-ils utilisés par les différents types de criminalité ? Ensuite, j'observe que l'époque n'est sans doute pas à la création de nouvelles agences, mais pourriez-vous revenir sur votre proposition d'agence technique ou nous faire parvenir une note à son propos ? Enfin, quelles sont vos suggestions pour nous, législateurs ?

M. Jérôme Notin. Les différents rapports existants en matière de cybersécurité, qu'ils soient parlementaires ou émanant de la Cour des comptes, font état d'un émiettement des dispositifs, préjudiciable à leur bonne compréhension sur

le terrain. Les victimes ne perçoivent pas les différences entre la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos), le service Perceval et le traitement harmonisé des enquêtes et signalements pour les e-escroqueries (Thesee). À la demande du président de la République, nous avons travaillé collectivement à la mise en place du 17cyber.gouv.fr, qui a vocation à orienter la victime vers tous les dispositifs étatiques, les prestataires historiques référencés et labellisés cybermalveillance.gouv.fr. L'activité de cybercriminalité ne va cesser de croître et nous militons pour faire du 17Cyber la solution visible.

Madame la rapporteure, l'impact de NIS 2 sur le GIP dépendra en grande partie des métiers que nous exerçons. D'après ce que j'en comprends, 0,5 % des entreprises et des collectivités seront concernées par NIS 2, soit une masse assez faible par rapport à la masse que nous traitons quotidiennement sur la partie assistance. S'agissant de la prévention, même si l'Anssi sera leur point de contact, nous serons ravis de fournir aux opérateurs d'importance vitale nos supports de sensibilisation.

Ensuite, comme je l'ai indiqué un peu plus tôt, nous éprouvons des difficultés à fidéliser les prestataires labellisés. Ils doivent consacrer du temps aux procédures que nous leur demandons, à nous transmettre les rapports d'incidents, les rapports de sécurisation. Les candidats doivent également verser 800 euros à l'Association française de normalisation (Afnor). À cet égard, France Cybersecurity labellise un éditeur de solutions cyber, mais il ne garantit pas que son détenteur soit en capacité d'évaluer la maturité cyber d'une structure, publique ou privée, et d'émettre des recommandations.

La plupart des RSSI travaillant dans les structures privées consacrent beaucoup de temps à remplir des tableurs pour démontrer leur conformité à des règles que chaque donneur d'ordre, public ou privé, établit lui-même. NIS 2 sera à ce titre extrêmement positif, puisque grâce à l'Anssi, il existera un référentiel technique commun sur lequel chacun pourra s'appuyer et des structures conformes à NIS 2 seront en mesure d'accompagner les acteurs.

Mme Johanna Brousse. Madame la rapporteure, vous m'avez interrogée sur l'intérêt d'utiliser le canal judiciaire comme une voie diplomatique. Quand nous signifions à un pays que nous avons mis en lumière son attaque et notamment l'utilisation de telle ou telle adresse IP, telle ou telle infrastructure, il s'aperçoit qu'il n'est plus du tout furtif et anonyme. Cela impliquera pour lui de devoir redéployer de nouvelles infrastructures pour pouvoir mener d'autres attaques. Il devra donc se réorganiser, ce qui lui fera perdre du temps et des moyens.

Ensuite, il existe au niveau de l'Anssi un dispositif très utile qui permet à des hackers éthiques de réaliser des signalements, ce qui dispense l'Agence de procéder à un article 40 ou à un signalement au parquet. Néanmoins, si nous sommes saisis par une entité qui a été hackée par un hackeur éthique, même agissant pour de bonnes raisons, à l'instar d'un lanceur d'alerte, nous serons malgré tout obligés d'ouvrir une enquête et il n'est pas exclu que la victime se constitue partie

civile auprès d'un juge d'instruction ou effectue une citation directe. Dès lors, il n'existe pas de véritable protection en tant que telle. Si l'on voulait pousser plus loin la protection des lanceurs d'alerte, il faudrait stipuler que ce hacking « éthique » constitue une cause d'exonération de la responsabilité pénale, ce qui n'est pas le cas à l'heure actuelle, même si le parquet reste maître de l'opportunité des poursuites.

Néanmoins, pour en avoir discuté récemment à Anssi, je sais que les acteurs de l'écosystème sont parfois réticents à signaler un événement, car ils redoutent d'encourir une responsabilité. Dès lors, il conviendrait peut-être de clarifier le dispositif, ce que je laisse à votre appréciation. Les personnes qui effectueraient des signalements légitimes devraient peut-être pouvoir disposer d'un cadre extrêmement protecteur et être incités à le faire.

Ensuite, nous constatons effectivement une réelle porosité. Les cybercriminels sont avant tout des mercenaires qui peuvent se mettre au service de certains États afin de mener à bien leurs actions. Régulièrement, des acteurs du rançongiciel travaillent directement pour des États, dans la mesure où le but du *ransomware* consiste certes à gagner de l'argent et à financer certaines opérations, mais aussi à entraver l'économie d'un pays.

Par ailleurs, le parquet national antiterroriste dispose d'un référent cyber avec lequel nous dialoguons. Des questions demeurent en suspens, néanmoins. Par exemple, si demain une cyberattaque de nature terroriste occasionne des morts, quelle sera la section chargée du dossier ? Il existe certes un plan de gestion de crise qui nous permet dans une certaine mesure de répondre à cette question. Mais peut-être conviendrait-il d'aller plus loin et de prévoir une possibilité de co-saisine de juridictions spécialisées, ce qui n'est pas le cas aujourd'hui.

Enfin, vous m'avez questionnée sur la proposition de création d'une agence technique pour le ministère de la justice et le ministère de l'intérieur. Différentes branches, ANTENJ et le SNCJ, existent aujourd'hui et effectuent un travail remarquable. Leur regroupement au sein d'une même agence dotée d'une mission globale et plus étendue permettrait de gagner en efficacité. Je pourrais vous transmettre un certain nombre d'éléments à ce sujet.

M. Christophe Husson. Depuis 2022, nous avons effectué 2 029 diagnostics sur les collectivités territoriales, dont trente étaient ultramarines et une sur onze avait été victime de rançongiciel. La plus petite était la mairie d'une commune de 200 habitants. Le dispositif a été étendu au PME ou aux ETI, qui s'est traduit par 338 diagnostics (dont neuf sur des entreprises ultramarines), dont une sur six avait été victime d'attaque par rançongiciel. Enfin, soixante-quatorze diagnostics ont été réalisés sur des hôpitaux en zone gendarmerie, dont un sur six a été victime d'un rançongiciel. Ces chiffres montrent bien qu'aujourd'hui, tout le monde est vulnérable, quelles que soient la structure et sa taille.

S'agissant de la gouvernance, notre entité est jeune au sein du ministère de l'intérieur et l'objectif consiste bien à assurer une meilleure coordination avec les

services enquêteurs de la police et de la gendarmerie. Je partage avec Jérôme Notin l'idée que le 17Cyber doit constituer le point d'entrée, lisible pour tous.

Le dispositif MonAideCyber de l'Anssi a été conçu comme une communauté d'aidants dans les territoires, qui pourra mener des diagnostics. Il convient de promouvoir cette communauté : plus nous disposerons de personnes en mesure de mener un diagnostic MonAideCyber dans les territoires, plus les modalités de prévention seront efficaces.

S'agissant du blanchiment des cryptomonnaies, le Comcyber de la gendarmerie a démantelé il y a quelque temps la plateforme Bitzlato et a saisi près de 20 millions d'euros en cryptomonnaies. Cette expérience est utile pour le travail de formation que nous menons, notamment au sein de notre centre de formation cyber de Lille. En effet, nous ne formons pas uniquement des spécialistes au niveau central à l'Office anti-cybercriminalité, à l'Unité nationale cyber ou la Brigade de lutte contre la cybercriminalité ; nous formons également des militaires de la gendarmerie et des fonctionnaires de la police nationale dans les territoires. En effet, nous avons besoin de personnes qui maîtrisent les sujets de la traçabilité des cryptoactifs, au plus proche des territoires en métropole et en outre-mer. De fait, ayant échangé à de nombreuses reprises avec des procureurs dans les territoires, je confirme qu'il existe aujourd'hui un véritable besoin de proximité.

Le rapport sur l'état de la menace est public. Il sera publié et disponible sur le site du ministère de l'intérieur, mais je vous le transmettrai dès sa publication. S'agissant du partage de l'information et en particulier le renseignement d'intérêt cyber avec les autres acteurs, le Comcyber-MI est connecté à l'InterCERT. Ici, le partage de l'information intervient en matière de captation de données et, potentiellement, de leur transmission.

J'ajoute que nos relations avec le Comcyber des armées sont très régulières. Le Comcyber-MI dispose ainsi d'un officier de liaison au sein du Comcyber des armées. Des rencontres bilatérales interviennent par ailleurs tous les six mois avec mon homologue au sein du ministère des armées. Nos équipes échangent très régulièrement sur le renseignement d'intérêt cyber. Nous disposons au Comcyber-MI d'une plateforme de Cyber Threat Intelligence (CTI) et nous éclairons le Comcyber des armées, qui conduit un projet sur le sujet. Nous travaillons évidemment de manière commune sur les difficultés et les pratiques et l'échange de l'information *stricto sensu*.

Enfin, une question a porté sur la reconnaissance faciale. À ce titre, je rejoins les propos initiaux qui ont concerné l'accès à la donnée. Aujourd'hui, la société est particulièrement numérisée ; nous disposons d'images vidéo statiques ou dynamiques. Dans le cadre d'une enquête judiciaire, une reconnaissance faciale pourra toujours constituer un élément utile pour les enquêteurs, notamment par son exploitation à l'aide de l'intelligence artificielle. Naturellement, ceci doit toujours intervenir dans un cadre légal adapté et garant de nos principes démocratiques.

M. le président Philippe Latombe. Je vous remercie de votre présence et d'avoir répondu aux questions.

La commission se réunira début septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer à notre réflexion et produire un texte le plus lisible et efficace possible. L'objectif consiste en effet à éviter des effets de bord.

11. Audition de Mme Laure de La Raudière, présidente de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) et M. Olivier Corolleur, directeur général de l'Autorité, mardi 8 juillet 2025 à 18 heures

Lors de sa réunion du mardi 8 juillet 2025, la commission spéciale a auditionné Mme Laure de La Raudière, présidente de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) et M. Olivier Corolleur, directeur général de l'Autorité.

M. le président Philippe Latombe. Je souhaiterais tout d'abord évoquer le calendrier d'examen du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. La commission spéciale l'examinera à partir du mardi 9 septembre. L'examen en séance publique est, à ce stade, prévu au début de la session extraordinaire qui devrait s'ouvrir le lundi 22 septembre.

Nous poursuivons nos auditions en recevant la présidente et le directeur général de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep).

Le Panorama de la cybermenace 2024 de l'Agence nationale de la sécurité des systèmes d'information (Anssi) illustre la diversité et la gravité des menaces qui pèsent, entre autres, sur le secteur des télécommunications. Cette étude distingue les menaces à visée lucrative, celles qui ont une finalité d'espionnage et celles qui visent à déstabiliser nos sociétés, les actes de sabotage relevant de cette dernière catégorie. Ainsi, l'Anssi a traité en 2024 la compromission et le chiffrement par le biais d'un rançongiciel d'une entité du secteur des télécommunications. Fait marquant de 2024, certaines rares attaques par déni de service distribué (DDOS) d'ampleur visant des infrastructures de télécommunications ont eu des conséquences importantes sur la disponibilité de services critiques. L'Anssi remarque également que le « ciblage d'opérateurs de télécommunications à des fins d'espionnage est intense ». Ces deux dernières années, l'Agence a ainsi traité plusieurs incidents affectant des entités du secteur des télécommunications en France à des fins d'espionnage.

Le projet de loi que la commission spéciale est chargée d'examiner comporte trois titres. Le titre I^{er}, consacré à la résilience des activités d'importance

vitale, procède à la transposition de la directive sur la résilience des entités critiques (REC). Mme Catherine Hervieu en est la rapporteure. Le titre II vise à renforcer notre cadre juridique en matière de cybersécurité et procède à la transposition de la directive NIS 2, relative à la sécurité des réseaux et des systèmes d'information. Sa rapporteure thématique est Mme Anne Le Hénanff. Enfin, le titre III est consacré à la résilience opérationnelle numérique du secteur financier et procède à la transposition du règlement sur la résilience opérationnelle numérique du secteur financier, dit Dora. M. Mickaël Bouloux en est le rapporteur. M. Éric Bothorel, quant à lui, est le rapporteur général du projet de loi.

Mme Laure de La Raudière, présidente de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Je suis accompagnée d'Olivier Corolleur, directeur général de l'Autorité, et de Virginie Mathot, ma conseillère à la présidence.

Dans le cadre de notre saisine pour avis sur le projet de loi, nous nous sommes concentrés sur les mesures qui s'appliquent spécifiquement au secteur que nous régulons, à savoir celles qui ont trait à la transposition de la directive NIS 2, à l'accès aux fréquences par les terminaux satellitaires terrestres et aux sanctions contre les auteurs de brouillages qui créent un préjudice. Nous nous sommes penchés notamment sur les questions qui pourraient avoir un impact, d'une part, sur le bon fonctionnement des réseaux et des services de communications électroniques, d'autre part, sur la sécurité juridique dont doivent bénéficier les opérateurs dans la mise en œuvre de leur obligation légale.

En comparaison de NIS, la directive NIS 2 s'applique à un éventail beaucoup plus large d'opérateurs : l'ensemble d'entre eux, quelle que soit leur taille, sont concernés – je ne parle pas des opérateurs d'importance vitale (OIV), qui sont couverts par le secret-défense et dont l'Arcep n'a pas à connaître. Dans le cadre de NIS, seuls les fournisseurs de DNS (systèmes de noms de domaine) et les points d'échange internet (IXP) étaient susceptibles de relever du périmètre des acteurs régulés au titre des opérateurs de services essentiels.

Dans le cadre de NIS 2, on parle d'entités essentielles et d'entités importantes – la catégorisation dépendant notamment de leur taille – mais tout le secteur des communications électroniques est concerné. Parmi les secteurs que nous régulons figurent les fournisseurs de services d'informatique en nuage, qui font partie du secteur hautement critique des infrastructures numériques et qui seront assujettis aux obligations de NIS 2, au même titre que les entités des services postaux et du courrier.

Les entités concernées se caractérisent donc par leur très grande diversité : dans le secteur que nous régulons, la directive s'applique à de très grands groupes comme à des entreprises de toute petite taille. À cet égard, nous appelons votre attention sur l'exigence de proportionnalité énoncée par la directive et rappelée par le Sénat à l'article 14 du projet de loi. Nous estimons qu'elle devrait être appréciée finement, en cohérence avec les moyens réels des entités assujetties.

Nous souhaitons également insister sur le délai de mise en conformité. Celle-ci nécessite en effet un effort substantiel en raison de l'ampleur des adaptations requises pour de nombreux acteurs. C'est valable pour les entités nouvellement assujetties – je pense aux très petites, petites et moyennes entreprises (TPE-PME), qui sont généralement les moins matures en matière de cybersécurité – mais cela peut aussi concerner les OIV ou les anciens opérateurs de services essentiels. Le champ d'application de NIS 2 étant beaucoup plus étendu que celui de NIS, c'est l'ensemble des systèmes d'information de l'entreprise qui sont concernés et non pas les seuls systèmes informatiques des infrastructures numériques sensibles.

C'est pourquoi, dans notre avis, nous avions appelé le gouvernement à prévoir une entrée en vigueur différée du projet de loi afin de laisser le temps aux acteurs de se conformer aux exigences de la nouvelle réglementation. Le gouvernement et le Parlement n'ont pas, pour l'instant, donné suite à cette demande. Toutefois, nos échanges avec l'Anssi ont mis en lumière le fait que l'Agence tiendrait compte de la capacité réelle des entités soumises à NIS 2 à respecter les obligations définies par le texte.

Nous avons aussi relevé des difficultés dans les critères d'assujettissement prévus par le projet de loi, notamment pour les entités implantées dans plusieurs pays ou qui y exercent différentes activités. Sur ce point, le projet de loi se borne à reprendre les critères de la directive sans apporter de précision, ce qui laisse perdurer des incertitudes. L'Anssi a indiqué que les textes réglementaires y répondraient en partie et qu'il était préférable de leur laisser le soin de préciser cette question, ce qui me paraît de bonne pratique.

Nous ne sommes pas directement concernés par NIS 2 puisque c'est l'Anssi qui mettra en œuvre la directive mais je voulais vous alerter sur l'ampleur de ce changement pour le secteur que nous régulons, laquelle variera néanmoins selon la taille des acteurs.

M. Éric Bothorel, rapporteur général. Le manifeste de l'Arcep commence par ces mots : « Les infrastructures numériques que sont les réseaux d'échanges internet, télécoms fixes, mobiles, les centres de données, ainsi que les réseaux postaux et de distribution de la presse, constituent des "infrastructures de libertés". Liberté d'expression et de communication, liberté d'accès au savoir et de partage, liberté d'entreprise et d'innovation qui sont autant d'enjeux clés pour le développement économique et la cohésion de notre pays au sein de l'Europe. » Je tiens à saluer ces termes car j'entends surtout parler, en ce moment, d'interdiction, de contrôle, de sanction et de surveillance – certes légale. Comment l'Arcep contribuera-t-elle, dans le cadre de nos débats, à ce que nous œuvrions à la résilience des infrastructures « de libertés » ?

Vous avez produit, en mai, une note intitulée « La résilience des réseaux de communications électroniques », dans le cadre de votre cycle de réflexion

« Réseaux du futur », dans laquelle vous mettez en exergue trois familles de risques : les risques organisationnels, technologiques et naturels.

Parmi les risques organisationnels, vous relevez notamment la fragmentation des acteurs impliqués dans l'exploitation des réseaux de communications électroniques. Du point de vue de l'Arcep, cela a-t-il un impact sur la cybersécurité ? Comment travaillez-vous sur ces questions ?

Compte tenu de l'émergence de nouveaux acteurs impliqués dans l'exploitation d'infrastructures de communications électroniques – je pense en particulier aux TowerCo (Tower Companies) et aux fournisseurs d'offres Telco Cloud –, vous préconisez une revue des obligations pesant sur l'ensemble des acteurs impliqués afin de s'assurer que celles-ci sont appropriées et proportionnées à l'objectif de sécurisation et de résilience. Le cas échéant, vous suggérez d'adapter et de préciser les règles. De votre point de vue, le projet de loi comporterait des lacunes : il ne garantirait pas que tous les opérateurs supportent bien les mêmes obligations. Pourriez-vous apporter des précisions à cet égard ?

S'agissant des risques technologiques, vous soulignez que « la virtualisation et la programmation logicielle des réseaux sont à l'origine d'une mutation profonde des architectures des opérateurs ». C'est un point de vue pertinent, sachant que le projet de loi évoque les infrastructures. Je vous cite encore : « Plus précisément, cette ouverture permet à des tiers (sociétés de services, fournisseurs d'applications, clients industriels /verticaux, MVNO, etc.) d'instancier et d'orchestrer eux-mêmes des services virtualisés. Elle implique donc que de nouveaux acteurs auront accès à certaines données et fonctions liées à l'exploitation du réseau, notamment celles de configuration et de souscription – ce qui relève du suivi de performance, de la supervision et de la maintenance du réseau devrait *a priori* rester sous contrôle exclusif de l'opérateur de réseaux ». À cet égard, des évolutions législatives vous paraissent-elles nécessaires, y compris pour renforcer vos compétences ?

Enfin, concernant les risques naturels, j'ai lu avec intérêt les développements que vous consacriez à l'organisation, aux moyens mis en œuvre et aux retours d'expérience en matière de gestion de crise. Vous citez un passage de la note d'analyse de France Stratégie intitulée « Risques climatiques, réseaux et interdépendances : le temps d'agir » : « les réseaux d'électricité, de transports routier et ferroviaire et de télécommunications […] sont associés, en fonctionnement normal comme en temps de crise, par de nombreux liens de dépendance, physiques ou découlant des relations entre les acteurs. » L'Arcep a-t-elle des recommandations à formuler concernant la gestion de crise et, plus spécifiquement, l'interdépendance des réseaux électriques et de télécommunications ?

Mme Laure de La Raudière. Je voudrais rappeler que l'Arcep est un régulateur économique qui intervient *ex ante* sur les marchés. Autrement dit, nous surveillons les marchés et regardons s'ils présentent des dysfonctionnements sur le plan concurrentiel et si les acteurs se conforment aux principes dont nous devons,

de par la loi, contrôler le respect. Nous imposons aux opérateurs, dans un cadre précisément défini, le respect d'obligations d'intérêt général – relatives à l'aménagement du territoire, à la concurrence, à l'innovation, etc. Il s'agit de faire en sorte que les acteurs privés se conforment à ces principes, au-delà de leurs intérêts propres.

Le traitement des enjeux de sécurité et de cybersécurité est de la responsabilité du gouvernement et non de l'Arcep. Comme l'importance que prennent internet et les réseaux sociaux dans la vie sociale et économique ne cesse de croître, nous avons souhaité, en tant qu'experts des télécoms, mettre ce sujet à l'ordre du jour des travaux du comité des réseaux du futur. Le comité réfléchit de manière prospective à certains thèmes qu'il fait exister dans le débat public. L'Arcep n'agit pas dans ce domaine en tant que régulateur économique mais comme expert au service du débat public. L'Autorité a publié en mai une note intitulée « La résilience des réseaux de communications électroniques », puis a organisé, avec la direction générale des entreprises (DGE), un webinaire pour la présenter aux collectivités territoriales. L'objectif est de réfléchir ensemble aux actions à déployer pour conforter la résilience des réseaux. Le comité peut également se pencher sur des sujets relatifs à la cybersécurité, puisque la résilience est aussi celle des réseaux face aux attaques informatiques.

Nous avons soulevé la question de la virtualisation des réseaux : ces derniers intègrent progressivement des logiciels et des fournisseurs différents, lesquels fragilisent les architectures antérieures. Nous alertons ceux qui seront chargés de déployer la directive NIS 2 ainsi que les opérateurs, sur la nécessité de mener un travail fin de détection des nouvelles fragilités des réseaux.

M. le président Philippe Latombe. Des représentants du secteur des télécommunications nous ont fait part, lors d'une audition, de leur souhait d'obtenir des éclaircissements sur le règlement Dora. Les entités soumises à cette norme peuvent diligenter des audits auprès de leurs fournisseurs critiques, dont font partie certains opérateurs de télécommunications.

Ils souhaitent limiter le champ du règlement sur deux points. Tout d'abord, ils veulent que les audits des systèmes d'information ne portent que sur la partie critique de ceux-ci. Ensuite, ils demandent à pouvoir refuser un auditeur pour éviter qu'un cabinet étranger accède à des informations critiques et sensibles. Partagez-vous leurs requêtes ?

Mme Laure de La Raudière. Limiter les audits à la seule partie critique des systèmes d'information me semble logique. Pourquoi les acteurs soumis au règlement Dora auraient-ils besoin d'avoir accès aux services clients ou facturation ? Aux opérateurs de télécommunications de prouver l'étanchéité de leurs systèmes d'information. Il est normal d'auditer la composante qui pilote le cœur du réseau et les équipements de télécommunications qui rendent le service et non celle centrée sur les ressources. L'Anssi est la mieux placée pour répondre à la question, notamment sur le plan technique.

Il pourrait être opportun d'autoriser un tiers à refuser un auditeur pour des raisons tenant à sa nationalité. Cela étant, l'entreprise auditée est forcément juge et partie, donc il faut trouver un dispositif équilibré. Il convient de protéger les audités du risque d'espionnage ou de fuite d'informations vers les concurrents : les auditeurs doivent respecter une déontologie forte et un acteur extérieur pourrait être chargé de contrôler cette obligation. Le sujet est néanmoins éloigné des compétences de l'Arcep.

M. Olivier Corolleur, directeur général de l'Arcep. Dans la note que vous avez citée, monsieur le rapporteur général, nous pointions principalement la modification de l'organisation du secteur. Ce dernier était animé par quelques opérateurs nationaux ; les responsabilités étaient partagées entre les opérateurs d'infrastructures, les acteurs commerciaux et les fonds d'infrastructures. Notre action consiste à déployer de manière pertinente un dispositif : pour ce faire, il faut bien connaître l'organisation afin de choisir judicieusement les opérateurs d'importance vitale et de définir des obligations générales.

Nous n'identifions pas de lacune dans la directive NIS 2. Pour les raisons que la présidente a exposées dans son propos liminaire, nous ne connaissons pas précisément les choix effectués dans le champ des opérateurs d'importance vitale. Nous devons prendre en compte les bouleversements de l'organisation du secteur dans la désignation des opérateurs les plus sensibles. Le cadre juridique est très complet pour les opérateurs de communications électroniques.

M. Vincent Thiébaut (HOR). Comment évaluez-vous, à l'échelle européenne, le risque lié à notre faible production de matériels d'infrastructures, sachant que les systèmes d'infrastructures utilisés par les opérateurs peuvent presque jouer le rôle de cheval de Troie ?

M. Éric Bothorel, rapporteur général. Les échanges d'informations et de courrier sont couverts par le principe du secret de la correspondance. La loi du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, dite loi « 5G », a rénové ce dispositif. Le Sénat a inséré dans le texte que la commission spéciale est chargée d'examiner une disposition relative à la protection du chiffrement. Jugez-vous cette mesure utile et nécessaire ?

Mme Laure de La Raudière. Monsieur Thiébaut, toute notre économie est exposée au risque de voir des équipements non européens utilisés sur nos réseaux. La question dépasse largement le champ des opérateurs de communication. Je défends la possibilité de privilégier les offres souveraines pour les services les plus critiques. Le rôle de l'Arcep est d'ouvrir les marchés numériques. Ces ouvertures permettent à des acteurs émergents d'apparaître, mais il faut s'assurer que ces derniers offrent des solutions de niveau et de qualité suffisants pour les entreprises. À l'échelle européenne, il convient de donner aux entreprises souveraines accès aux marchés publics. Les marchés privés sont très concurrentiels et les entreprises peuvent avoir peur de tester des solutions par peur de perdre des parts de marché si

leur modèle n'est pas le plus avancé ; même si l'exigence de qualité de service est élevée pour les citoyens, les marchés publics sont moins compétitifs, donc ils représentent un domaine intéressant. Dans le secteur des télécoms, deux équipementiers, Ericsson et Nokia, sont européens, donc nous bénéficions d'une certaine protection. Dans une loi qui devait s'appeler la loi Bothorel, on a fait en sorte que tous les équipementiers utilisés par nos opérateurs de télécommunications respectent certaines règles et soient habilités par l'Anssi.

Sur le secret des correspondances, nous sommes très attachés au chiffrement. C'est à la représentation nationale de décider du cadre juridique de celui-ci. L'absence de chiffrement ou l'accès aux clés de chiffrement fragilisent la protection des correspondances.

M. le président Philippe Latombe. Je vous remercie d'avoir répondu à nos questions.

12. Table ronde sur le chiffrement réunissant des représentants de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT), du groupement interministériel de contrôle (GIC) et de la direction générale de la sécurité intérieure (DGSI), mercredi 9 juillet 2025 à 14 heures

Lors de sa première réunion du mercredi 9 juillet 2025, la commission spéciale a procédé à l'audition, ouverte à la presse, puis à huis clos, de M. Mahamadou Diarra, secrétaire général de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) ; M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC) ; et Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI).

M. le président Philippe Latombe. Dans le cadre de nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, nous allons traiter du chiffrement, sujet particulièrement important que nous n'avions pas encore abordé et sur lequel nous souhaitions avoir l'éclairage de la communauté du renseignement. Cette audition et la suivante seront entièrement consacrées à l'examen de l'article 16 *bis* du projet de loi, de ses implications concrètes et de son insertion dans le corpus législatif.

Disons-le d'emblée, si la question du chiffrement est importante, il n'était pas évident qu'elle trouve sa place dans le débat sur ce projet de loi au regard des dispositions de l'article 45 de la Constitution et du contrôle qu'en effectue le Conseil constitutionnel. Mais le Sénat ayant adopté un amendement d'Olivier Cadic, président de la commission spéciale, cet article 16 *bis* est désormais dans la navette parlementaire et il nous revient de l'examiner avec toute l'attention qu'il mérite.

La question du chiffrement avait fait l'objet de débats animés lors de l'examen de la loi du 13 juin 2025 visant à sortir la France du piège du narcotrafic.

Dans sa formulation actuelle, l'article 16 *bis* dispose : « Il ne peut être imposé aux fournisseurs de services de chiffrement, y compris aux prestataires de services de confiance qualifiés, l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques tels que des clés de déchiffrement maîtresses ou tout autre mécanisme permettant un accès non consenti aux données protégées. »

M. Mahamadou Diarra, secrétaire général de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT). Vous souhaitez disposer de l'éclairage de la communauté du renseignement sur cet article 16 *bis.* Dans le propos introductif dont j'ai été chargé, je vais vous présenter l'avis technique des services. Nous serons ensuite à votre disposition pour répondre à vos questions, sous réserve du respect du secret de la défense nationale. Nous pourrons entrer davantage dans les détails lors de la partie de l'audition qui se déroulera à huis clos, même si nous devons respecter les obligations qui s'imposent à nous.

Sur le fond, nous considérons que l'article 16 *bis* n'a pas sa place dans le projet de loi. Les services de renseignement sont confrontés au quotidien aux enjeux du chiffrement, évolution majeure de nos moyens de communication, qu'ils soient interpersonnels ou entre machines. Le chiffrement permet de sécuriser nos transactions bancaires, nos investigations sur internet, nos échanges de messages ou nos appels. C'est un élément essentiel de la politique française de cybersécurité, édicté dans la posture nationale sur le chiffrement. La mission des services de renseignements est de protéger la propriété intellectuelle de nos industries et de sécuriser les communications des autorités de l'État. Pour le dire simplement, le chiffrement concourt en tant que moyen technique à la sécurité des systèmes d'information de la nation.

Dans leur travail quotidien, les services de renseignements constatent que certains moyens, notamment les messageries chiffrées, sont utilisés par des personnes mal intentionnées. Il ne s'agit pas ici de pointer du doigt les opérateurs de messageries chiffrées qui ne sont que des outils, mais de rappeler que certains usages ayant des impacts sur la sécurité nationale se développent à l'aide de ces outils. Nous ne sommes pas les seuls à faire ce constat. Il me semble que Johanna Brousse, cheffe de la section de lutte contre la cybercriminalité du parquet de Paris, et le général Christophe Husson, chef du commandement du ministère de l'intérieur dans le cyberespace, ont pu vous le rappeler pour ce qui concerne le judiciaire.

Dans tous les pays européens, cette évolution préoccupante fait l'objet d'un constat partagé. En avril 2024, les chefs de police européenne ont alerté *via* Europol sur les risques associés au fait de voir se développer des espaces de non-droit sur les plateformes numériques grâce au chiffrement et ils ont appelé les industriels du numérique à trouver le juste équilibre entre vie privée et sécurité publique. Un rapport de juin 2024, corédigé par Europol et Eurojust, dresse un état des lieux technico-opérationnel factuel de l'impact du chiffrement au-delà des seules communications chiffrées. Ultime exemple, le groupe d'experts de haut niveau HLEG a rendu un rapport mettant en relief trois nécessités : préservation des

bénéfices du chiffrement pour nos sociétés ; transparence des entreprises du numérique en matière de données collectées ; coopération entre les États et les opérateurs pour mettre en œuvre des systèmes d'accès légal à leurs données, encadrés strictement par la loi et contrôlés.

La complexité du sujet – bénéfice du chiffrement et enjeux associés – implique de développer une approche nuancée, fondée sur un principe de proportionnalité. Rappelons le cadre d'action des services de la communauté du renseignement qui regroupe 20 000 agents au sein de dix services relevant de quatre ministères – intérieur, armées, justice, économie et finances. Consacrée par la loi du 24 juillet 2015, la politique publique de renseignement est fondée sur la défense et la promotion de sept intérêts fondamentaux de la nation, définis à l'article L. 811-3 du code de la sécurité intérieure, notamment la prévention du terrorisme et la prévention de la criminalité et de la délinquance organisées – ce sont les 4° et 6° dudit article.

Bénéficiant d'outils d'enquête importants dont nous sommes conscients, les techniques de recueil du renseignement (TRR), les services de renseignement font l'objet de mécanismes de contrôle stricts définis par le législateur, afin de s'assurer que ces outils sont utilisés dans le cadre défini par la loi et de manière proportionnée. La loi a ainsi institué la Commission nationale de contrôle des techniques de renseignement (CNCTR), composée de magistrats de l'ordre judiciaire et de l'ordre administratif ainsi que de parlementaires. Elle est systématiquement saisie pour avis par le premier ministre de chaque demande de techniques de renseignement et elle effectue un contrôle *a posteriori* sur pièces et sur place. Elle élabore chaque année un rapport public dont la dernière édition a été diffusée le 25 juin dernier. La délégation parlementaire au renseignement (DPR) est composée de quatre députés et quatre sénateurs habilités qui exercent la mission de contrôle parlementaire de la politique publique du renseignement. Son dernier rapport public date du 30 avril dernier.

Les services de renseignement doivent adapter leurs moyens d'action aux évolutions technologiques, comme il a fallu le faire par le passé avec l'apparition de la poste, du télégraphe ou des réseaux téléphoniques. Le principe de proportionnalité est au cœur du dispositif légal en vigueur à travers l'article L. 801-1 du code de la sécurité intérieure : « Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. »

Selon notre analyse, cet équilibre fondamental serait ébranlé par l'article 16 *bis* du projet de loi qui pourrait avoir des effets de bord au-delà de la seule consécration du chiffrement. Nous en concluons qu'il convient de laisser sa place au travail technique approfondi et exhaustif, qui prend du temps au regard de la technicité du sujet, afin d'englober les problématiques très différentes et de

restituer au gouvernement et au législateur un ensemble factuel leur permettant d'évaluer en toute connaissance de cause l'opportunité d'une évolution du dispositif légal. C'est ce qui occupe actuellement l'administration et singulièrement la communauté du renseignement. Étant donné la nature des droits en cause, aucune évolution ne se fera sans revenir devant le Parlement, ce qui garantit votre rôle majeur, votre office, dans toute éventuelle décision en la matière.

En résumé, les dispositions de l'article 16 *bis* nous interdiraient de réfléchir aux différentes options sur un sujet aussi central. *A contrario*, laisser à l'administration le temps de travailler permet de documenter plusieurs options. L'une d'elles consiste à apporter des réponses aux enjeux de sécurité posés par le chiffrement si et seulement si un équilibre et des garanties sont trouvées en termes de secret des correspondances et de sécurité des systèmes d'information. Autre option : ne pas donner accès aux communications chiffrées, mais prendre ces décisions en conscience sur la base d'un travail étoffé sur les plans juridique, technique et opérationnel, qui est en cours.

Laisser à l'administration le temps d'approfondir ses travaux permet d'éviter de prendre des initiatives à l'emporte-pièce, sous le coup de l'émotion, dans un sens ou un autre, ce qui est probablement le plus important. Il me semble que Nicolas Roche, secrétaire général de la défense nationale et de la sécurité nationale (SGDSN), a adopté cette même position lorsque vous l'avez auditionné, il y a quelques semaines.

M. Éric Bothorel, rapporteur général. Avant toute chose, je voulais remercier les hommes et les femmes des services qui concourent à la sécurité de nos concitoyens.

Vous avez donné votre opinion sur l'article 16 *bis*, mais nous ne manquerons pas de revenir sur le sujet car la porte est ouverte à des évaluations techniques permettant de concilier liberté et sécurité.

Comment adapter la sécurité informatique de la société aux vulnérabilités des appareils personnels ? De telles mesures pourraient-elles être introduites dans la loi ?

Comme la direction générale de la sécurité intérieure (DGSI) le souligne de temps à autre, le facteur humain est le principal vecteur de compromission des systèmes d'information, notamment au travers de la mauvaise utilisation d'une messagerie professionnelle. Comment remédier à ces cas de figure ?

En quoi consiste la réalisation d'investigations en sources ouvertes du premier niveau sur internet et les réseaux sociaux et dans le cadre de dossiers opérationnels d'évaluation de la menace par la DGSI ? Nous nous écartons là du chiffrement, mais nous nous intéressons aussi au renseignement d'origine sources ouvertes (Osint). Actuellement, la récupération de données volées constitue un recel en droit pénal. Ayant été attentifs à l'audition de Johanna Brousse et de Christophe Husson, vous n'ignorez pas que c'est un sujet qui nous préoccupe. Êtes-vous

favorables à l'idée de permettre une telle récupération pour un motif légitime ? Comment concilier à la fois le droit pénal, le droit de propriété intellectuelle, la protection des données à caractère personnel et la cybersécurité en ce qui concerne l'Osint ? Plus largement, quelle est votre opinion sur le recours à l'Osint pour améliorer la cybersécurité ?

Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI). Nombre de questions dépassent le cadre de l'article 16 *bis* et portent sur des modalités d'action ou de recueil de renseignement, que je préfèrerais aborder à huis clos.

Pour le reste, il s'agit de rechercher un équilibre entre la protection des libertés individuelles et collectives et ce qui relève de la sécurité nationale. Nous devons tenir compte des évolutions technologiques et ne pas remettre en cause les règles de sécurité numérique dont nous bénéficions sans réduire à néant l'efficacité des services de renseignement – qui relèvent de mon champ de compétences – et des services d'enquêtes judiciaires.

Depuis des décennies, l'État dispose légalement du droit d'intercepter des communications téléphoniques. Il l'exerce de façon ciblée dans un cadre administratif pour ce qui relève des techniques de renseignement ou dans un cadre judiciaire pour ce qui concerne les interceptions de sécurité. Les interceptions s'effectuent sous le contrôle de la CNCTR dans le cadre administratif et sous l'autorité d'un magistrat dans le cadre judiciaire. Tous les services du monde – de renseignement ou judiciaires – sont cependant confrontés à une réalité : l'usage de plus en plus développé des messageries chiffrées rend cette technique obsolète. En conséquence, nous perdons de la visibilité sur les activités criminelles des cibles, la détermination de leur projet criminel et, ce qui préoccupe le plus la DGSI, la préparation de leurs projets violents.

Pour schématiser la situation avec mes mots, c'est-à-dire selon une approche qui n'est pas nécessairement technique, je dirais que l'objectif auquel nous devons concourir dans le cadre des travaux évoqués, c'est de tenter de voir si nous pouvons étendre les pratiques que nous avons actuellement avec les opérateurs téléphoniques à d'autres opérateurs, les plateformes de messagerie chiffrées. Pourrions-nous agir dans les mêmes conditions d'exigence légale et de contrôle que celles qui existent pour les interceptions téléphoniques ou les écoutes judiciaires, selon le cadre dans lequel on se place ? Ce sont ces travaux qu'il nous faut poursuivre. Les mutations technologiques nous imposent de trouver un nouvel équilibre technique et juridique entre le secret des correspondances et la protection de la sécurité nationale. Si le choix était fait de ne pas retrouver cet équilibre, il faudrait au moins être en mesure de l'assumer, en en mesurant les conséquences techniques, politiques et, pour ce qui me concerne, opérationnelles.

M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC). En effet, tout est question d'équilibre en cette matière. Nous l'avons trouvé avec les opérateurs de communication électronique, entre nécessité

d'un accès et garantie de la protection de la confidentialité et de l'intégrité des communications. L'Agence nationale de la sécurité des systèmes d'information (Anssi) joue un rôle éminent à l'articulation entre ces deux mondes, l'article 226-3 du code pénal faisant la mesure entre les deux impératifs.

Tout est une question d'équilibre car les techniques de renseignement sont décidées par le premier ministre à la suite d'un examen de leur proportionnalité – l'atteinte au secret et à la vie privée versus l'impératif de sécurité nationale. Cet équilibre, que nous avons trouvé avec les opérateurs de communications électroniques, nous le cherchons encore avec les opérateurs d'extrémité ou lesdites plateformes.

Comment tout cela fonctionne-t-il ? Le GIC – et lui seul – adresse des réquisitions aux opérateurs de communications électroniques en application d'autorisations d'interception de sécurité prises par le premier ministre sur la base d'identifiants, c'est-à-dire des numéros de téléphone, des adresses IP ou n'importe quel sélecteur en fonction de l'autorisation délivrée et de l'utilisation qu'en fait la personne désignée dans l'autorisation. Les opérateurs de communications électroniques sont coopératifs avec les pouvoirs publics. Je profite d'ailleurs de l'occasion pour saluer les directions des obligations légales des opérateurs. Leurs agents sont soumis à des enquêtes de sécurité ; ils travaillent entourés de murs épais ; ils se rendent disponibles vingt-quatre heures sur vingt-quatre pour répondre aux réquisitions du GIC. Je les en remercie.

La suite, vous la connaissez : les opérateurs de communications électroniques se contentent désormais de transporter des flux qui leur sont impénétrables, car chiffrés de bout en bout. Ils dupliquent vers le GIC des communications chiffrées dont le chiffrement leur échappe puisqu'il est à la main des opérateurs d'extrémité ou des plateformes. Depuis les révélations d'Edward Snowden en 2013, le chiffrement s'est en effet généralisé. Il est activé par défaut. Nos logiciels nous alertent d'ailleurs par des pop-ups assez angoissants lorsqu'il n'est pas actif. Ce chiffrement des communications s'est traduit par une bascule économique majeure : les opérateurs de réseaux se sont trouvés privés de la valeur marchande que constituent nos données au profit des opérateurs d'extrémité qui les détiennent et qui en font un commerce lucratif.

Ces derniers connaissent, ou ont toute latitude pour connaître, notre vie privée et professionnelle – nous leur confions les deux. En revanche, les services de renseignement sont privés de leur outil de travail de base. Le législateur avait prévu en 2015, de façon encadrée, un recueil de données informatiques grâce auquel les services peuvent légalement récupérer le contenu des terminaux électroniques, là où les données sont en clair, conformément à l'article L. 853-2 du code de la sécurité intérieure. Or cette récupération est coûteuse et difficilement généralisable. C'est pourquoi la coopération des opérateurs de réseaux ou de transport ne suffit pas : il nous faut absolument celle des opérateurs d'extrémité, dits OTT, *over the top*, ou plateformes.

La coopération avec les opérateurs de réseaux fait l'objet de standards techniques. Elle est encadrée par l'article 226-3 du code pénal, et l'administration s'est organisée pour que tout fonctionne, au bénéfice des enquêtes judiciaires comme du renseignement. Les opérateurs sont dédommagés des surcoûts liés à leurs obligations, en application d'arrêtés tarifaires.

La coopération entre les pouvoirs publics et les plateformes existe, mais elle ne repose pas encore sur des standards techniques. Il n'y a d'ailleurs aucune offre industrielle d'interface normalisée pour accéder aux données des plateformes. Les textes d'application de l'article 226-3 du code pénal se concentrent sur les réseaux de transport. Si l'État s'est organisé pour ce qui est de la coopération avec les opérateurs de réseaux, il ne l'a pas encore fait de manière formelle s'agissant des plateformes, pour donner corps à la coopération. C'est un défi absolument considérable. Nous en sommes, pour l'instant, à examiner de grandes orientations, qu'il faudra ensuite confronter à la réalité de chaque service de communication de chaque plateforme. Nous pourrons ensuite trouver avec ces acteurs un intérêt commun à élaborer et adopter des standards. Tout cela nécessite un travail posé et approfondi, comme l'a indiqué Nicolas Roche devant votre commission. À ce stade, nous ne sommes pas en mesure de décrire une solution. De toute façon, il n'en existera pas qu'une : le *one size fits all* (taille unique) ne vaut pas dans ce domaine.

L'essor des technologies de communication nous facilite la vie, mais il facilite aussi grandement le crime, les violences collectives, l'espionnage et le terrorisme. L'article 16 *bis* du projet de loi a certes pour but d'affirmer le principe absolument fondamental de la protection de la vie privée, mais cela dans le cadre d'une loi technique, portant sur un mécanisme particulier, le chiffrement, et en exigeant de lui une propriété qui n'est pas indispensable à la protection de la vie privée. Ce texte érige, en fait, le chiffrement en totem, ce qui tuera dans l'œuf toute discussion avec les plateformes, alors que celle-ci est nécessaire pour préserver des capacités d'enquête essentielles, dans un domaine où prévaut la recherche d'une solution équilibrée, de proportionnalité entre atteinte à la vie privée et sécurité nationale. En transcrivant sans nuance dans la loi une position à la fois technique et radicale, on briserait un équilibre savamment entretenu par la Constitution, le législateur, jusqu'à présent, et l'autorité indépendante qu'est la CNCTR, au quotidien. C'est pour ces raisons que le gouvernement vous a demandé de supprimer l'article 16 *bis* et de lui laisser le temps de travailler sereinement, avec les plateformes, à des solutions équilibrées.

Que se passerait-il si la loi sanctifiait le chiffrement ? D'une part, cela reviendrait à annoncer aux criminels que les outils de communication de M. Tout-le-monde leur permettent de préparer en toute impunité leurs actes. Le seul moyen qu'il nous resterait pour pénétrer les communications des criminels serait de pénétrer leurs moyens de communication, conformément à l'article L. 853-2 du code de la sécurité intérieure, ce qui irait à l'encontre des intentions des auteurs de l'article 16 *bis* du projet de loi, puisque cela nous donnerait accès à plus de données que ce qui nous serait nécessaire. En prenant le contrôle d'un smartphone, on n'accède pas seulement aux communications, c'est-à-dire au flux, mais aussi aux

fichiers enregistrés, c'est-à-dire au stock, ainsi qu'aux brouillons, aux contacts, à l'appareil photo, au microphone, etc. Il en résultera donc automatiquement un effet pervers. Des techniques plus intrusives, que la loi réserve à des cas subsidiaires, lorsqu'aucun autre moyen n'est disponible, seront parfaitement justifiables sur le plan légal puisqu'il n'existera aucun autre moyen d'accéder aux communications. Par conséquent, au motif qu'on ne pourra pas accéder aux communications, on accédera potentiellement à bien plus.

D'autre part, la sanctuarisation du chiffrement augmentant la demande d'accès aux données en clair, une offre va se créer. Un autre équilibre prévaudra donc, celui de l'offre et de la demande. Nous verrons alors proliférer un secteur commercial lucratif, constitué de sociétés privées offrant des prestations ou des logiciels d'intrusion à des services de police judiciaire ou administrative. L'article 16 *bis* créera un business de la vulnérabilité et du hacking, dont nous devinons qu'il sera dominé par des acteurs dont nous ne voulons pas.

L'article 16 *bis* porte sur des moyens techniques, dont la place dans une loi peut être discutée. Il est absolutiste, puisqu'il ferait également tomber « tout autre mécanisme ». Le gouvernement, par la voix de la ministre chargée du numérique, a déjà alerté vos collègues sénateurs sur les effets de bord de cette disposition. L'article s'appliquera de façon indifférenciée aux enquêtes judiciaires et au renseignement et aura pour conséquence le développement d'un marché des vulnérabilités et du hacking, qui fera la part belle à des prestataires étrangers. Il conduira les services à mettre en œuvre des techniques de renseignement plus intrusives, plus attentatoires à la vie privée. Il percutera, par ailleurs, les réflexions en cours au niveau européen – la Commission s'est saisie du sujet, comme l'a rappelé le secrétaire général de la CNRLT. Cela signifie que l'adoption de cet article conduira la France à s'exclure de la démarche engagée par l'UE. Enfin, il ruinera la coopération entre l'État français et les plateformes, qu'il est susceptible de faire reculer.

Mme Anne Le Hénanff, rapporteure. Je rappelle, tout d'abord, que l'article 16 *bis* n'est pas apparu dans le texte par hasard : c'était une réaction d'un collègue sénateur, Olivier Cadic, à l'introduction surprise d'une disposition autorisant des *backdoors* (portes dérobées) dans la proposition de loi dite narcotrafic.

Vous nous demandez de vous laisser du temps, ce que je comprends totalement. Je n'ai pas, à ce stade, d'opinion sur l'article 16 *bis*, mais il me paraît bon de pouvoir discuter de ces questions dans le cadre du groupe transpartisan lancé par Florent Boudié – j'espère que vous y serez associés. Cela me paraît une bonne perspective temporelle.

Pouvez-vous préciser quelle est la part, parmi toutes les demandes d'accès aux données que vous adressez aux entreprises, de celles concernant la lutte contre la pédocriminalité et la lutte contre le narcotrafic ? Je crois savoir qu'elle est tout à fait négligeable, alors que la lutte contre le narcotrafic et la lutte contre la

pédocriminalité étaient les deux arguments principaux pour justifier l'introduction de l'article 8 *ter* dans la proposition de loi « narcotrafic ».

La technique dite du fantôme, qui permet à un utilisateur invisible de participer à une conversation sur une messagerie chiffrée, ne constitue-t-elle, de votre point de vue, ni une vulnérabilité informatique ni un affaiblissement du chiffrement ?

Quid du filtre de détection de contenus spécifiques mis en place par Apple, notamment pour ce qui est des contenus pédopornographiques échangés sur WhatsApp ou Messenger ?

Que répondez-vous à celles et ceux qui estiment que l'introduction d'une vulnérabilité informatique permettant aux services de l'État d'accéder au contenu des messageries chiffrées pourrait être exploitée par des puissances étrangères à des fins de cyberespionnage ?

Comment expliquez-vous que la gendarmerie nationale ait réussi à accéder au contenu des messages échangés entre des criminels sur le réseau chiffré EncroChat ?

Êtes-vous associés, de près ou de loin, aux discussions qui ont lieu au niveau européen dans le cadre de la stratégie de sécurité intérieure ProtectEU ?

M. Pascal Chauve. La pédopornographie ne fait pas partie des finalités légales du renseignement au sens de l'article L. 811-3 du code de la sécurité intérieure. Il n'existe donc pas de demandes reposant spécifiquement sur ce motif. Le dernier rapport annuel de la Commission nationale de contrôle des techniques de renseignement, évoqué par M. Diarra, rend parfaitement compte de ces questions : la prévention de la criminalité organisée représente 16,1 % des finalités poursuivies par les techniques de renseignement en 2024. Je suis incapable de vous dire la part exacte de la lutte contre le narcotrafic, mais il est certain que celui-ci est au cœur de la criminalité organisée, qui entretient des mafias brassant un argent absolument considérable et qui est susceptible de porter atteinte aux intérêts fondamentaux de la nation. C'est ce que recouvre, en très grande majorité, la sixième finalité de l'article L. 811-3 du code de la sécurité intérieure.

Mme Céline Berthon. En matière de renseignement, les finalités des réquisitions ne sont pas communiquées aux opérateurs. Dire pourquoi on s'intéresse à un numéro de téléphone – contre-terrorisme, contre-espionnage ou contre-ingérence – serait totalement contraire au principe de protection de l'activité de renseignement. Cela rend d'autant plus complexe l'identification précise des éléments en question.

M. Pascal Chauve. Cela protège non seulement l'enquête mais aussi la personne visée.

M. Mahamadou Diarra. Nous avons bien conscience du contexte dans lequel l'article 16 *bis* a été introduit, mais il me semble que l'article de la proposition de loi « narcotrafic » auquel vous avez fait référence n'a pas été adopté. Il constituait l'une des options possibles, avec l'article 16 *bis*.

Quand je demande de laisser du temps pour mener un travail de fond, c'est que les travaux en cours seraient entravés, ou en tout cas mis en difficulté, si cette disposition était adoptée. On aurait, en effet, tranché, de même que si d'autres dispositions étaient adoptées. La position de l'administration et des autorités dans la discussion avec les opérateurs serait extrêmement entravée.

Je confirme que les services de l'État sont impliqués dans les discussions européennes, la Commission s'étant saisie du sujet, notamment sous l'angle judiciaire, compte tenu des compétences qui sont les siennes. Nous participons à ces discussions, mais les travaux sur la doctrine de sécurité européenne, proposée par la Commission, en sont encore à leurs débuts.

La question de l'utilisateur fantôme fait partie du travail en cours sur les techniques qui pourraient permettre, ou non – nous partons du postulat que la discussion est ouverte –, d'avoir accès à des informations sans affaiblir le chiffrement. Il faudra que les administrations continuent d'y travailler pour que le gouvernement et le Parlement puissent, le moment venu, se reposer la question. Je n'ai pas à me prononcer sur des initiatives parlementaires, mais nous sommes prêts à concourir à la réflexion et à revenir devant vous si besoin.

Mme Catherine Hervieu, rapporteure. Je m'intéresse plus particulièrement à la nécessité pour les collectivités territoriales, les services publics et les entreprises de protéger leurs données, spécifiquement celles à caractère personnel, dans le cadre de leurs différentes activités. Pouvez-vous nous donner des éléments sur la manière dont ces acteurs sont accompagnés et conseillés face aux enjeux du chiffrement ?

M. Mahamadou Diarra. Le sujet de la protection fait l'objet d'une mobilisation de l'ensemble des acteurs, singulièrement le SGDSN, à travers l'Anssi. Vous avez parlé des collectivités territoriales, mais on pourrait également évoquer les hôpitaux, qui sont des acteurs sensibles, exposés aux enjeux concernant les données.

Des travaux de sécurité des systèmes d'information sont menés par l'Anssi. Son directeur général, que vous verrez prochainement, me semble-t-il, pourra y revenir. Par ailleurs, mais je m'exprime là sous le contrôle de ma collègue, les services de renseignement, la DGSI comme la DNRT, la direction nationale du renseignement territorial, mènent des actions de sensibilisation envers les entreprises et les acteurs publics, notamment les collectivités territoriales, au sujet des messageries, sous l'angle de la protection – ne pas se faire piéger, sécuriser ses données, éviter les mésusages des téléphones personnels et professionnels lorsqu'on manie des données sensibles. Tout un écosystème est mobilisé, au sein duquel

l'Anssi joue un rôle central, sous l'autorité du SGDSN et avec l'appui de la CNRLT et la mobilisation des services de renseignement sur le territoire national.

Mme Céline Berthon. Je crois qu'il ne faudrait pas prendre le risque de tomber dans une confusion entre, d'une part, ce qui relève de l'enjeu de la sécurité numérique générale, qui concerne la société dans son ensemble et doit nous conduire, eu égard à la place de l'outil informatique dans nos vies et dans les systèmes d'information de toutes les organisations, privées comme publiques, à intégrer des réflexes de sécurité numérique dans les comportements, y compris au sein des administrations publiques, des collectivités territoriales et des sociétés privées, dont un certain nombre sont effectivement couvertes et accompagnées par nous en matière de protection économique, et d'autre part ce dont il est question aujourd'hui, à savoir d'envisager et éventuellement d'accepter techniquement la construction d'un dispositif qui soit légalement autorisé, contrôlé et dirigé sur certaines personnes qui seraient des cibles au titre des finalités poursuivies, dans un cadre administratif ou judiciaire.

Les dispositifs que nous évoquons à demi-mot n'ont pas vocation à s'appliquer à M. et Mme Tout-le-monde. Nous en avons besoin pour les missions qui nous sont confiées en matière de protection de la sécurité nationale ou des intérêts fondamentaux de l'État, dans le domaine du renseignement, ou en matière de lutte contre les phénomènes majeurs de crime organisé qui ont été évoqués. Le rapport annuel de la Commission nationale de contrôle des techniques de renseignement illustre à quel point les mesures de surveillance technique que nous pourrons être amenés à mobiliser dans les services de renseignement français couvrent un nombre limité de personnes, dans un cadre réglementaire et légal très strict et extrêmement contrôlé *a priori* et *a posteriori*.

Je comprends tout à fait les enjeux de sécurité numérique qui s'appliquent à tous ; notre propos est d'essayer de vous convaincre de l'importance d'avoir un débat serein et le plus rationnel possible, afin de ne pas priver les appareils sécuritaires, judiciaires ou de renseignement d'un moyen de travailler de manière très ciblée sur des gens qui sont des dangers soit pour la sécurité nationale soit pour le vivre-ensemble en France.

M. Thomas Gassilloud (EPR). Je remercie les sénateurs de nous donner l'occasion d'échanger sur le chiffrement, même si tel n'est pas le premier objet du projet de loi.

Quelles sont les pistes qui s'offrent à nous, aux échelons national et européen, pour résoudre le problème ? Quel est le degré de coopération des messageries instantanées en matière d'accès ciblé à tel ou tel service ?

Quelles sont, hors de l'Union européenne, les modalités de coopération entre les autorités et ces messageries ? Certains États ont-ils imposé l'implantation de *backdoors* – portes dérobées – ou l'accès massif et automatisé à certaines données des messageries instantanées ?

Par ailleurs, vos observations étayent la nécessité de disposer d'une messagerie instantanée européenne. Ce sujet est-il à l'ordre du jour de la discussion avec nos collègues européens ?

M. René Pilato (LFI-NFP). Qui donne les ordres ? Est-il normal ou gênant que l'ordre vienne du premier ministre ? Faut-il opter pour une personnalité indépendante ou neutre ou pour des fonctionnaires du ministère de la justice ? Qui vous donne l'autorisation ?

La possibilité de déverrouiller un chiffrement au nom de la sûreté de l'État ne me pose aucun problème. Ce que je souhaite, c'est savoir qui décide quoi lorsque vous avez repéré quelque chose qui peut tourner mal. J'aimerais que nous discutions de la question de savoir qui, lorsqu'il s'agit de sécurité nationale, doit être habilité à donner les ordres quand vous détectez quelque chose de dangereux, afin de prévenir toute dérive politique, quelle que soit la personne au pouvoir.

M. Vincent Thiébaut (HOR). J'aimerais savoir, très naïvement, comment vous analysez l'impact sur la sécurité intérieure de vos difficultés à accéder à certaines données d'outils de messagerie, alors qu'aux États-Unis, leurs éditeurs agissent dans le cadre de la législation américaine « Cloud Act » qui leur impose des engagements auprès de l'État fédéral.

Mme Céline Berthon. La mise en œuvre des techniques de renseignement obéit à une procédure strictement encadrée par la loi du 24 juillet 2015 relative au renseignement. Elle prévoit notamment que, pour avoir recours à des techniques de renseignement, les services doivent émettre des demandes, qui sont préalablement examinées par la CNCTR, dont les membres sont notamment issus du haut de la hiérarchie de la juridiction administrative et de l'autorité judiciaire ainsi que du Parlement.

Elle se prononce de manière collégiale sur les techniques qui lui sont soumises. Son avis est transmis à l'autorité politique. Il incombe au premier ministre, sur cette base, d'autoriser ou non la mise en œuvre des techniques visées.

Par ailleurs, la loi fixe une liste limitative et précise des techniques et des finalités. Selon les domaines, les moyens sont mobilisables en totalité ou désignés de façon très limitative. Leur utilisation est bornée dans le temps.

Il s'agit donc d'une procédure très carrée, inscrite dans un cadre légal très clair. La CNCTR exerce son contrôle avec finesse et exigence. Elle n'autorise pas toujours la mise en œuvre des techniques demandées et rend compte de ses refus, de façon très transparente, dans son rapport annuel – le plus récent a été publié en avril dernier.

M. René Pilato (LFI-NFP). Si je comprends bien, la CNCTR est neutre et indépendante, mais le premier ministre peut passer outre son avis.

M. Pascal Chauve. Dans le processus qui vient de vous être décrit, la demande est formulée par un service, endossée par un ministre et visée par la CNCTR. C'est bien le premier ministre qui décide – il ne saurait, dans notre pays, en aller autrement dans ce domaine.

Si le premier ministre décide de passer outre l'avis négatif de la CNCTR et d'autoriser la mise en œuvre d'une technique de renseignement, le Conseil d'État est saisi de façon automatique, ce qui offre une garantie supplémentaire. L'alignement entre la commission et l'autorité décisionnaire est impératif, sous peine de déclencher un mécanisme très complexe, que n'avons jamais dû activer, de saisine du Conseil d'État contre le premier ministre.

M. Mahamadou Diarra. Tout cela démontre la reconnaissance dont jouit la CNTCR auprès des autorités.

S'agissant des questions des membres de la commission, il nous sera impossible d'y apporter une réponse précise, même à huis clos.

M. Pascal Chauve. Je dirai, pour atténuer la frustration des membres de la commission spéciale, que nous avons choisi, en France, un système de supervision effective des techniques de renseignement. Le législateur a confié à la CNCTR un pouvoir énorme, en lui offrant un accès permanent, complet et direct aux renseignements recueillis et à ce que les services de renseignement en font.

J'ai l'honneur de diriger un service centralisant les techniques de renseignement pour le premier ministre, qui peut ainsi vérifier que les services de renseignement ont bien agi dans les limites qu'il a fixées dans son autorisation et dans les décisions qu'il a prises. Cette centralisation bénéficie à la CNCTR, qui peut exercer son contrôle *a posteriori* en disposant, comme le prescrit la loi, d'un accès permanent, complet et direct aux données.

M. Éric Bothorel, rapporteur général. Ce n'est pas parce que j'ai été l'un des artisans de la lutte contre l'article 8 *ter* de la proposition de loi sur le narcotrafic que je suis un fan absolu de l'article 6 *bis* en question. J'ai plutôt un avis assez tranché sur le fait que l'on ne répond pas aux excès d'une proposition de loi par les excès d'un projet de loi. À ce titre, je comprends les éléments que vous avez détaillés.

Vous dressez le constat qu'il est nécessaire d'opter pour une réponse technique faute de parvenir à collaborer avec les plateformes. N'aurions-nous pas pu parvenir à une telle collaboration grâce à un dialogue renforcé par l'intermédiaire d'outils tels que le groupe de contact permanent (GCP) ? Créé au lendemain des attentats de janvier 2015, il s'est réuni à de multiples reprises en 2015 et en 2016, très peu en 2017 et en 2018 et pour la dernière fois en 2019. Cette instance, à laquelle sont associées les plateformes, pourrait être un lieu de délibération des évolutions technologiques des uns et des autres ainsi que du rôle de chacun. Sa réunion régulière a été proposée après les émeutes urbaines de l'été 2023.

Je suis surpris que l'on dresse le constat définitif selon lequel nous ne parviendrons pas, par la collaboration, l'échange et le droit, à obliger les plateformes à collaborer et à participer à des coopérations judiciaires de même niveau que celles auxquelles participent les opérateurs téléphoniques au motif que les uns sont nationaux et les autres ne le sont pas. Le droit européen devrait nous aider à y parvenir, ainsi que des instances ne relevant pas du droit dur, telles que le GCP. Je fais partie de ceux qui s'étonnent que l'on fasse peu de cas du GCP, qui, à ses débuts, a porté ses fruits, et qui est désormais abandonné. Quel est votre sentiment à ce sujet ?

Mme Céline Berthon. Nous vous répondrons à huis clos.

*
* *

La commission spéciale a ensuite auditionné, à huis clos, MM. Mahamadou Diarra, secrétaire général de la coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) ; M. Pascal Chauve, directeur du groupement interministériel de contrôle (GIC) ; et Mme Céline Berthon, directrice générale de la sécurité intérieure (DGSI).

En raison du huis clos, la teneur des propos tenus au cours de cette réunion ne donne pas lieu à une retranscription écrite, ni à un enregistrement accessible depuis le portail vidéo de l'Assemblée nationale.

13. Table ronde sur le chiffrement réunissant des entreprises et des experts de la cryptographie, mercredi 9 juillet 2025 à 15 heures

Lors de sa deuxième réunion du mercredi 9 juillet 2025, la commission spéciale a auditionné sous la forme d'une table ronde, ouverte à la presse, MM. Thomas Baignères et Matthieu Finiasz, docteurs en cryptographie, co-fondateurs de la société Olvid et M. Benjamin Beurdouche, chercheur en ingénierie de sécurité et de confidentialité chez Mozilla.

M. le président Philippe Latombe. Nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité concernent aujourd'hui la question du chiffrement.

Cette audition est entièrement consacrée à l'examen de l'article 16 *bis* du projet de loi, de ses implications concrètes et de son insertion dans le corpus législatif. La commission spéciale n'avait pas encore abordé ce sujet lors de ses auditions.

Si la question du chiffrement est importante, il n'était pas évident qu'elle trouve sa place dans le débat sur ce projet de loi au regard des dispositions de l'article 45 de la Constitution et du contrôle qu'en effectue le Conseil

constitutionnel. En tout état de cause, cet article est désormais dans la navette et il nous revient de l'examiner avec toute l'attention qu'il mérite.

M. Benjamin Beurdouche, chercheur en ingénierie de sécurité et de confidentialité chez Mozilla. Je remercie la commission pour son invitation à discuter d'un sujet aussi complexe et important que celui de la résilience de la nation et en particulier de l'impact de la cryptographie dans cet écosystème.

Je suis chercheur en cryptographie chez Mozilla, titulaire d'un doctorat de cryptographie et méthodes formelles de l'École normale supérieure (ENS) et spécialiste de la conception, de l'analyse et de l'implémentation des protocoles cryptographiques.

Je suis l'un des co-auteurs de TLS (*Transport layer security*), principal protocole utilisé pour sécuriser internet et le *web*, et de l'un des nouveaux protocoles qui vont être utilisés pour protéger les communications audio-vidéo et pour la téléphonie mobile.

Je vais centrer mon propos sur les aspects relatifs à la cryptographie, mais suis à votre disposition pour échanger sur les questions plus larges de cybersécurité.

La menace qui pèse sur nos sociétés dans le monde numérique est multiforme. La connectivité et la numérisation permettent de grands progrès technologiques et sociétaux, mais rapprochent aussi chaque jour la menace des attaquants au plus proche de nos infrastructures critiques et des populations française et européenne. Il faudra donc être de plus en plus vigilant.

Dans ce contexte, la transposition des directives REC (Résilience des entités critiques), NIS 2 (*Network and Information Security*) et la réglementation Dora (Digital Operational Resilience Act) sont extrêmement importantes. Il est nécessaire que la loi prévoie un cadre minimal rigoureux pour l'ensemble des acteurs, mais définisse aussi une ligne directrice permettant aux acteurs les plus proactifs de mener l'effort efficacement sans se trouver confrontés à des incertitudes juridiques. De nombreux efforts ont déjà été effectués et sont en cours pour protéger les utilisateurs des services numériques des entreprises de la BITC (base industrielle et technologique de cybersécurité), dont je considère que Mozilla fait partie. Il faut toutefois que cette démarche soit poursuivie par l'ensemble de l'écosystème économique et pas uniquement par le secteur numérique.

Ces directives visent à rehausser le niveau de sécurité des entités les plus critiques. Les sénateurs ont jugé opportun d'ajouter au titre II un article 16 *bis* afin de sanctuariser les outils les plus fondamentaux de cette sécurité, c'est-à-dire la cryptographie.

La cryptographie est l'outil principal qui nous permet de créer de la confiance dans l'intégrité, la confidentialité et l'authentification de nos données, peu importe le moyen, qu'elles soient en transit au sein de communications ou stockées sur des systèmes pour emploi futur. Il est extrêmement important de se

rendre compte que cette pierre angulaire protège nos transactions financières, les communications du gouvernement, des institutions, des services d'urgence, de la sécurité opérationnelle de nos forces armées, de nos journalistes et est utilisée pour la diplomatie. Elle est donc absolument critique.

Il faut également être conscient que la moindre vulnérabilité dans un système cryptographique est dans une certaine mesure démultipliée par rapport à une faiblesse que l'on introduirait dans un système de sécurité informatique classique, car elle est systémique. La cryptographie étant une pierre angulaire, chaque atteinte qui lui est portée affaiblit le dispositif de sécurité de manière très systématique. Il est donc extrêmement important de veiller à prévenir les fragilités susceptibles d'intervenir silencieusement comme dans n'importe quel système d'information et d'être utilisées contre des journalistes, des opposants politiques, des forces de l'ordre, voire dans des situations plus courantes de violences conjugales ou domestiques.

D'un point de vue technique, je pense que l'article 16 *bis* est une bonne chose puisqu'il renforce la sécurité. Nous pourrions toutefois discuter la terminologie utilisée, notamment l'emploi du mot « chiffrement » en lieu et place du terme « cryptographie ». En effet, le chiffrement renvoie uniquement à la confidentialité, tandis que la cryptographie concerne également l'intégrité et l'authentification.

J'ai noté par ailleurs au chapitre IV, titre II, article 38 une révision des articles 30 et 35 du titre III de la loi pour la confiance dans l'économie numérique (LCEN) sur l'importation et l'exportation des moyens cryptologiques, qui a été introduite par le Sénat. Cela va dans le bon sens, mais doit sans doute être encore discuté.

Je souhaiterais clarifier un point qui ne me semble pas toujours suffisamment visible dans la position des chercheurs notamment. Nous n'avons pas de position idéologique sur le chiffrement, seulement une vision technique. Je comprends tout à fait les problématiques de sécurité défense, qui me sont assez familières, et les besoins opérationnels exprimés auparavant. Toutefois, je ne pense pas qu'il y ait de problématique particulière, si ce n'est la capacité d'accéder aux outils existants. Nous disposons en effet déjà d'outils ciblés qui nous permettent par exemple de faire du renseignement, des techniques d'enquête spéciales et tout ce dont nous avons besoin.

En revanche, il existe peut-être un problème de réorganisation des moyens de l'État pour définir qui y a accès, pour quels besoins, etc. Sans doute vaudrait-il mieux, au lieu de systématiser l'affaiblissement du chiffrement, aller vers l'emploi de ces outils ciblés en replaçant les moyens situés par exemple au ministère des armées vers de l'interministériel, ce qui permettrait au ministère de l'intérieur d'avoir également accès à ce type d'outils dans le cadre de sa lutte contre la criminalité du haut du spectre. On pourrait ainsi imaginer une discussion entre le président de la République chef des armées et le premier ministre sur la désignation

de la priorité stratégique à donner à chaque typologie de cible et les moyens à y consacrer, sans affecter la pierre angulaire que constitue le chiffrement. Selon moi, moins on touche au chiffrement, mieux on se porte.

En conclusion, je suis favorable à l'article 16 *bis*. Une cryptographie solide est bien évidemment nécessaire, mais reste insuffisante. Il convient d'envisager également l'ensemble des problématiques de sécurité des systèmes d'information qui s'y rattachent, dont NIS 2, Dora et REC essaient de faire monter le niveau.

M. Thomas Baignères, cofondateur de la société Olvid. Matthieu Finiasz et moi représentons la société Olvid, qui développe la messagerie éponyme. Nous en sommes respectivement CTO (*Chief Technology Officer*) et CEO (*Chief Executive Officer*). Nous faisions partie de l'équipe qui a développé le projet et sommes tous deux docteurs en cryptographie, la science du secret.

Notre objectif avec Olvid était de permettre à tous d'avoir accès à un moyen de communication sur internet. Nous sommes évidemment très directement touchés par le projet de loi et en particulier par l'article 16 *bis*. Nous souhaitons avant tout partager ici notre avis d'experts en cryptographie. Il ne s'agit pas simplement de défendre les intérêts de notre société. Le sujet est bien trop important pour se contenter de défendre son pré carré.

Sur le fond, l'article 16 *bis* nous semble, tel que nous le comprenons, très positif : c'est une excellente chose que d'écrire noir sur blanc que la France refuse de se voir imposer des *backdoors* dans des systèmes de chiffrement et d'affirmer que la cybersécurité en France ne sera pas intrinsèquement plus faible que celle d'autres pays. On peut effectuer un parallèle avec le RGPD (règlement général sur la protection des données), qui avait permis aux utilisateurs européens de voir leurs données mieux protégées, faisant de l'Europe une exception par rapport au reste du monde. Il serait dommage qu'une directive européenne imposant un affaiblissement du chiffrement vienne à nouveau faire de l'Europe une exception, mais dans l'autre sens.

Nous sommes, chez Olvid, favorables à l'idée défendue par l'article 16 *bis*. Toutefois, cela ne nous empêche pas d'être à l'écoute de l'ensemble des parties prenantes et en particulier des forces de l'ordre. Notre objectif est aussi de comprendre leurs problématiques. Leur travail est évidemment fondamental et il est de notre devoir de prendre en compte leur point de vue dans notre réflexion. Notre conviction est que seul un dialogue dépassionné, scientifique et précis permettra d'apporter une solution mesurée à ces problématiques de fond. C'est la raison pour laquelle nous nous tenons à votre disposition, ainsi qu'à celle de toutes les parties prenantes, pour répondre de façon aussi transparente que possible à l'ensemble des questions soulevées par ce sujet si sensible.

M. Éric Bothorel, rapporteur général. Vous succédez à d'autres organisations qui n'ont pas tenu exactement le même discours que vous sur

l'article 16 *bis*, dont je pense qu'il n'est pas forcément écrit comme il devrait l'être et qu'il peut être compromettant pour l'avenir. Nous aurons l'occasion d'y revenir.

Concernant les recommandations d'usage de la messagerie Olvid, savez-vous si la circulaire du 22 novembre 2023 est respectée ? Pensez-vous qu'il faille l'étendre à d'autres organismes publics ? Vous aviez alors bénéficié d'une belle exposition grâce à l'exécutif. Quels sont selon vous les obstacles au développement de messageries instantanées chiffrées dites souveraines ? Comment réduire la dépendance aux applications les plus connues du grand public et, de manière plus générale, aux grands éditeurs de logiciels américains ?

A-t-on vraiment d'autres choix, lorsque les plateformes refusent de coopérer avec les autorités françaises, que d'imaginer des dispositifs venant compromettre le chiffrement ? Cet enjeu, majeur, est au cœur de nos débats. Force est de constater que certains acteurs ne veulent pas coopérer. Or cette coopération semble indispensable pour recueillir des informations et pouvoir mener des actions allant parfois jusqu'à l'interpellation. Comment procéder lorsque les plateformes refusent de coopérer ?

M. Matthieu Finiasz, cofondateur de la société Olvid. Intégrer dans la loi des règles imposant une *backdoor* pour permettre de déchiffrer des communications ne changera pas forcément grand-chose, car si les plateformes refusent de coopérer, elles ne le feront pas davantage pour la *backdoor*.

Cela soulève un premier problème de fond : comment s'assurer que les plateformes partagent avec les autorités, c'est-à-dire au moins avec la police et la gendarmerie, les données auxquelles elles ont déjà accès ? Il s'agit d'un problème de coopération. Une société qui propose une messagerie instantanée va-t-elle par exemple donner accès à tous ses logs, à toutes les données qu'elle a collectées grâce aux différents moyens à sa disposition dans cette opération ? Apparemment, certaines messageries coopèrent très bien, d'autres pas du tout. L'arrestation de Pavel Dourov était, me semble-t-il, liée à cela.

Un second problème, très différent, se pose ensuite : veut-on obliger les plateformes à fournir plus que les données auxquelles elles ont accès pour créer leur service ? Cela va à l'encontre du RGPD et de tous les dispositifs visant, en Europe, à protéger la vie privée. Cette collecte doit-elle par ailleurs être systématique pour tout le monde ou ciblée sur certains individus ? Les forces de l'ordre souhaitent évidemment qu'elle soit ciblée. La question est de savoir s'il est techniquement possible d'effectuer une collecte de données ciblée, sur demande, sans que cela n'implique une collecte généralisée des informations de l'ensemble des usagers. Mon point de vue est qu'une collecte ciblée n'est pas forcément possible techniquement. Cela signifie en effet que le système doit affaiblir le chiffrement, la cryptographie et la sécurité en général pour tout le monde, afin de pouvoir de temps en temps piocher dans un nouveau pool de données que l'on aura forcé des opérateurs à collecter afin d'en extraire quelques informations. Cela conduit à affecter le niveau de sécurité de l'ensemble d'une solution.

Lorsque nous avons conçu la messagerie, l'un des objectifs de base d'Olvid était, par opposition à toutes les autres messageries, de rendre impossible toute attaque de masse sur notre solution. La cryptographie d'Olvid a été conçue pour qu'il n'y ait jamais de tiers de confiance obligatoire pour tous les utilisateurs. Cela signifie que si l'on veut récupérer des données d'un utilisateur, il faut s'attaquer spécifiquement à lui, à son téléphone, à son ordinateur. Il n'est pas possible de les collecter en un seul point commun à tous les utilisateurs, comme un serveur de distribution de messages ou autres dispositifs de ce type. Cela fait partie des fondements qui ont présidé à la création d'Olvid. Toute tentative de mise en place de mesures permettant de collecter les données de tout le monde en un point unique irait à l'encontre de cette démarche et viendrait abaisser le niveau de sécurité.

M. Thomas Baignères. Ces mesures imposeraient nécessairement abaisser le niveau de sécurité car on ne sait pas *a priori*, au moment où l'on conçoit la solution, quelles personnes on pourrait être amené à cibler. Cela suppose donc que les moyens à déployer pour cibler une personne six mois après la conception du système soient intégrés d'emblée pour l'intégralité des utilisateurs. Il faut nécessairement mettre en place un dispositif qui touche tout le monde afin de pouvoir l'activer *a posteriori*. Il ne sera pas possible selon nous de réaliser un ciblage réellement fin ; le dispositif concernera nécessairement tout le monde, dès le départ, avec un abaissement général du niveau de sécurité.

La directive de Mme Borne nous a effectivement été très bénéfique. Certaines sociétés en France font l'effort de développer des solutions pas simplement prétendument sûres, mais qui démontrent leur niveau de sécurité, par du code open source et de la documentation technique expliquant le code et permettant aux personnes chargées d'en effectuer l'audit de le faire dans les meilleures conditions. Il est désormais possible, grâce à l'Anssi (Agence nationale de la sécurité des systèmes d'information), de passer en France des CSPN (certifications de sécurité de premier niveau). Nous ne sommes pas les seuls à l'avoir fait. Il nous semblerait naturel de mettre en avant toutes les sociétés qui font cet effort et engagent des fonds pour aller au bout du processus et démontrer leur qualité.

Mme Anne Le Hénanff, rapporteure. Pouvez-vous préciser en quoi le fait d'intégrer un système donnant *a priori* la capacité au service de cibler une personne six mois plus tard le fragilise ?

Quel est par ailleurs le type de données demandé par les services de l'État et dans quelle mesure y répondez-vous ? Certains services de l'État indiquent que des entreprises refusent de transmettre des données auxquelles elles ont pourtant accès tout en acceptant de les fournir aux services américains.

Dans quelle mesure la technique dite de l'utilisateur fantôme, qui permet à un utilisateur invisible de participer à une conversation via une messagerie cryptée, ne constitue-t-elle selon vous ni une vulnérabilité informatique ni un affaiblissement du chiffrement ?

Je souhaiterais enfin vous entendre sur l'enjeu spécifique de la cryptographie post-quantique. On entend dire en effet que le système quantique fera disparaître toute protection de messagerie cryptée. Est-ce un mythe ou une réalité ?

M. Benjamin Beurdouche. La technique de l'utilisateur fantôme est un affaiblissement d'un protocole cryptographique qui sous-entend que l'on ajoute dans les destinataires légitimes d'une communication sécurisée un tiers invisible par les utilisateurs. Cela n'est possible que dans certains cas. Cette technique affaiblit le but de sécurité qui veut qu'une communication chiffrée ait pour destination une cible définie, constituée d'individus bien particuliers. Le recours à l'utilisateur fantôme étend cette cible de manière anormale et rompt les propriétés de sécurité du protocole et du système. Cette rupture des promesses de sécurité peut s'effectuer au niveau du protocole cryptographique ou de l'application, qui peut utiliser le protocole correctement mais être activement malicieuse et contourner le chiffrement. De manière générale, cela n'est possible que dans le cas où le protocole cryptographique ne construit pas la propriété de consensus sur les participants au groupe.

Dans les protocoles modernes, notamment ceux qui vont être déployés dans les téléphones mobiles Android IRC (*Internet Relay Chat*) et iOS (*iPhone Operating System*) pour la prochaine génération de messageries chiffrées, le protocole ne permet pas d'ajouter des participants invisibles. L'application peut toujours tricher, mais le protocole cryptographique en lui-même prend des dispositions en ce sens.

Tout est possible, mais cela revient à réduire la sécurité du système et à donner potentiellement un accès aux données, puisqu'il faut ajouter la personne fantôme : qui l'ajoute ? Comment procéder de manière ciblée ? Autant de questions auxquelles on ne peut pas répondre, puisque lorsque l'on distribue un logiciel de manière générale à toute la population, soit on affaiblit le système d'emblée, avec une réserve qui fait que toute personne en ayant connaissance peut utiliser cette faiblesse, soit on procède de manière active, ciblée, avec des outils offensifs – ce qui est à mon avis beaucoup plus sûr. Mais autant, en réalité, ne pas le faire et attaquer directement le terminal de la personne. Une démarche offensive ciblée est préférable à une vulnérabilisation de l'ensemble des utilisateurs.

Il existe, en matière de cryptographie post-quantique, une problématique de transition post ordinateurs quantiques. Depuis plusieurs années, nous déployons, lors de la conception des logiciels de sécurité des protocoles de communication, notamment pour internet, des protocoles dits hybrides, qui protègent contre les ordinateurs classiques et quantiques. Cela existe depuis très longtemps pour les sites de très haute valeur ajoutée comme internet, avec le protocole HTTPS (*Hypertext Transfer Protocol Secure* ou protocole de transfert hypertexte sécurisé), les transactions financières, etc. Si vous utilisez par exemple Firefox, il faut savoir que 20 % environ de vos connexions se déroulent dans le cadre d'un protocole protégeant contre l'apparition d'un ordinateur quantique.

L'idée est que les attaquants collectent les messages chiffrés transitant sur internet en essayant par exemple de cibler une ambassade non protégée contre le post-quantique et dont ils savent que le diplomate va, à une heure donnée, passer un appel. Quand un ordinateur quantique suffisamment fort pour casser la cryptographie apparaîtra, il sera capable de déchiffrer les communications collectées jusqu'alors. Si nous sommes actuellement incapables d'estimer quand cet ordinateur apparaîtra, nous sommes en revanche scientifiquement convaincus qu'il arrivera. Nous prenons donc depuis plusieurs années déjà des dispositions visant à protéger tous nos protocoles de première classe en hybridant le système, c'est-à-dire en incluant à la fois de la cryptographie classique et de la cryptographie résistant à un ordinateur quantique, afin de sécuriser rapidement le maximum de cas d'usage.

Cela s'avère toutefois très compliqué, notamment dans les déploiements de matériel qui prennent souvent beaucoup de temps, parfois des décennies. Á titre d'exemple, le dernier gros déploiement cryptographique effectué sur internet remonte à 2018, lors de la conception du protocole précédemment évoqué. Or en 2025, il apparaît que 70 % seulement des personnes cibles utilisent la dernière version du protocole. Cela signifie donc que 30 % des gens utilisent des protocoles vieux de parfois vingt ou trente ans. Dans ce contexte, il est très important que les règlementations NIS 2 ou Dora insistent sur l'effort quantique qu'il convient d'effectuer. Cela s'annonce critique. Il est donc essentiel de commencer le plus tôt possible.

M. Matthieu Finiasz. Il est important de savoir qu'il existe déjà des algorithmes cryptographiques post-quantiques capables de résister aux ordinateurs quantiques ; encore faut-il les intégrer dans les différents logiciels. Olvid dispose d'une certification Anssi et il est question que l'Agence impose à tous les produits certifiés d'avoir une résistance post-quantique, donc du chiffrement hybride, afin de conserver leur certification. Nous allons progressivement travailler sur ce point. Nous n'avons pas intégré cet élément dès l'origine, car lorsque nous avons conçu la cryptographie d'Olvid, les protocoles en question n'étaient pas complètement standardisés. Des standards existent dorénavant, sur lesquels nous pouvons nous appuyer, considérant que, tout le monde ayant les mêmes standards, le système devrait résister.

Cela ne signifie pas que les ordinateurs quantiques vont arriver demain – bien malin qui pourrait dire quand apparaîtra un ordinateur quantique capable de casser réellement la cryptographie. Nous savons en tout cas nous en protéger en cas de besoin. Il ne restera qu'à effectuer le déploiement et la mise à jour des protocoles, afin d'effectuer la bascule d'un univers cryptographique classique sujet à des attaques d'ordinateurs quantiques vers une cryptographie hybride post-quantique.

Sur des systèmes comme TLS pour du chiffrement de sessions web, c'est assez simple parce qu'il n'y a pas forcément beaucoup de persistance dans le temps. Il s'agit de protocoles qui ont été conçus pour prévoir des évolutions au cours du temps. Dans les cas de systèmes hardware, rien n'est parfois prévu et il faut changer les puces. Dans du logiciel, cela va souvent plus vite.

Olvid a été conçu pour ne jamais avoir un point de faiblesse face à une attaque de masse de tous les utilisateurs en un seul coup. L'utilisateur fantôme, c'est exactement cela. En gros, c'est un moyen applicable à n'importe quel utilisateur, qui va permettre de récupérer le contenu de ses communications parce que ses messages vont partir vers un utilisateur fantôme. Donc dans les cas où on peut mettre en place cet utilisateur fantôme, on peut générer une attaque de masse. Le problème, c'est que ce qui déclenche cette attaque de masse, ce n'est pas de la cryptographie.

Quand on fait un protocole cryptographique entre plusieurs utilisateurs, on a une preuve scientifique que si les conditions d'application du modèle de sécurité sont respectées, la sécurité va tenir. C'est une preuve scientifique. Dans un système avec utilisateur fantôme, on n'a plus de preuve scientifique et il faut alors se demander comment protéger l'accès avec le déclenchement de l'ajout. On sort complètement du cadre de la cryptographie. Il y a quelque part dans un bureau quelqu'un qui a un bouton lui permettant d'activer l'utilisateur fantôme pour telle personne. Ce n'est plus de la cryptographie, ce n'est plus de la science et il est difficile de mesurer l'impact que cela peut avoir. Ce qui est sûr, c'est que cela a un impact négatif sur la sécurité. Dans le cas où l'application de l'utilisateur fantôme n'est pas sélective, le problème est le même : comment contrôler l'accès au pool de données ? Ce n'est plus de la cryptographie, c'est de la sécurité standard, physique, pour empêcher l'accès aux disques durs sur lesquels se trouvent les données. C'est précisément ce que nous voulons absolument éviter. La sécurité de la cryptographie de notre système est scientifiquement prouvée et nous ne voulons pas retomber dans un dispositif à l'ancienne avec des informations cachées dans un cahier placé au fond d'un coffre-fort. Ce serait dommage de revenir à cela au XXI^{e} siècle.

M. le président Philippe Latombe. Récemment, le gouvernement fédéral américain a demandé aux fonctionnaires fédéraux de ne plus utiliser une certaine application de messagerie chiffrée au bénéfice d'une autre, jugée plus sûre. Ces questions de chiffrement, de déchiffrement et d'affaiblissement du chiffrement traversent-elles selon vous de la même façon toutes les sociétés démocratiques ? Si c'est le cas, les réponses sont-elles les mêmes ?

Les sénateurs, lors de l'examen du projet de loi sur la cybersécurité, ont ajouté un article 16 *bis*, en réaction à un amendement adopté lors des débats sur la loi contre le narcotrafic qui visait à affaiblir le chiffrement. Avez-vous été associés, en tant que spécialistes de la cryptographie, à la réflexion globale menée à l'époque par le ministère de l'intérieur ? Le ministre de l'intérieur nous avait expliqué, lors des débats, que l'utilisateur fantôme ne représentait pas un affaiblissement du chiffrement.

M. Thomas Baignères. La question se pose clairement de manière globale. Elle s'est posée aux États-Unis et une première réponse a été apportée. Selon moi, celle-ci ne sera pas la même partout. Nous verrons la réponse qui sera apportée en France, mais elle sera potentiellement différente de celle des États-Unis. Le RGPD

est un dispositif profondément européen. L'état d'esprit ici est différent de celui de pays plus lointains.

Non, nous n'avons pas été consultés préalablement aux réflexions scientifiques, notamment sur l'utilisateur fantôme. Nous avons participé au débat, de manière un peu précipitée, alors que c'était quasiment déjà trop tard, si j'ose dire. Nous avons été pris au dépourvu.

Je reviens sur la question de l'utilisateur fantôme. Certes, nous sommes passionnés par les mathématiques derrière le chiffrement ; elles sont en effet suffisamment belles pour qu'on s'y intéresse. Cela étant, je comprends que la plupart des gens s'intéressent, non pas au chiffrement en lui-même, mais aux garanties de confidentialité, d'authenticité et d'intégrité qu'il apporte. Or avec une solution comme l'utilisateur fantôme, ces garanties ne sont plus nécessairement présentes. Certes, mathématiquement, elle ne touche pas au chiffrement et notamment pas à l'algorithme AES (*Advanced Encryption Standard)*, qui est utilisé majoritairement, mais, en envoyant des messages en clair à une autre source, le chiffrement lui-même est contourné. La question est donc de savoir, non pas si on touche au chiffrement, mais si on continue à garantir la confidentialité, l'authenticité et l'intégrité des communications. Le chiffrement n'est pas une fin en soi : c'est un moyen d'apporter ces garanties. De notre point de vue, une solution telle que l'utilisateur fantôme affaiblit nécessairement les communications de tous ceux qui utilisent des systèmes comme le nôtre.

M. Benjamin Beurdouche. D'un point de vue scientifique, quand on conçoit un système de sécurité informatique, on part des propriétés de sécurité de la session de télécommunication, par exemple la confidentialité, l'authentification et l'intégrité. Si un attaquant est présent dans une session, par exemple en raison d'un malware installé sur le téléphone, on va jouer son jeu au niveau des primitifs cryptographiques, au niveau des protocoles cryptographiques, au niveau des applicatifs, puis vers les infrastructures pour arriver jusqu'à internet. La cryptographie n'est que le moyen d'obtenir les garanties de confiance attendue du système, notamment ces trois propriétés.

Tout le monde doit faire face aux mêmes problématiques. Les recommandations de changement d'outils de sécurité pour les communications viennent du fait que les applicatifs sont maîtrisés par différentes parties. Tout le monde est d'accord pour dire que la cryptographie doit être solide, mais l'effort de sécurité doit être fait pour chaque couche. Olvid est maîtrisé par une entreprise de confiance et son système peut donc être utilisé pour des informations de plus haut niveau de sensibilité. Signal a un très bon protocole, mais l'application est opérée aux États-Unis. Un système *open source* permet de vérifier qu'il se comporte comme il est censé se comporter. Même si le code est fait pas un ensemble hétérogène de personnes de différentes nationalités, il est possible de vérifier, grâce à l'ouverture du code, les propriétés de sécurité de ce dernier. Dans un système de messagerie, on ne fait pas confiance à l'infrastructure et on fait donc en sorte qu'elle

voie le moins de choses possible. Une messagerie souveraine nécessite donc des infrastructures souveraines aux niveaux français et européen.

Personnellement, je ne connais aucun collègue qui aurait été auditionné au préalable sur l'article 8 *ter*, sur les *backdoors*, sur les propriétés de sécurité ou sur les objectifs des forces de sécurité intérieure et du ministère de l'intérieur. Je plaide pour une discussion ouverte avec le ministère de l'intérieur et les services de renseignement au niveau purement technique. Je pense que nous sommes tous à disposition.

Mme Anne Le Hénanff, rapporteure. Considérez-vous, déontologiquement, qu'une demande des services de sécurité intérieure, encadrée par la justice et ciblée, entraînerait nécessairement une vulnérabilité ? Les messageries sont utilisées par des trafiquants notamment. Est-il dès lors possible de hiérarchiser ? Face à l'évolution de la menace, envisagez-vous d'évoluer dans votre approche de la cryptographie ?

M. Thomas Baignères. La menace n'est pas dans la question qui nous serait posée, car nous avons pleine confiance dans notre système démocratique. Nous sommes à la disposition des forces de l'ordre pour discuter de manière générale des propriétés du chiffrement ou sur des cas particuliers. Notre inquiétude porte sur notre capacité à développer un système qui conserve les mêmes propriétés de sécurité que nous sommes aujourd'hui en mesure d'offrir tout en leur permettant d'avoir accès à certaines données d'un système de messagerie comportant l'échange de message avec des métadonnées. Nous sommes aujourd'hui dans l'incapacité scientifique d'ouvrir de manière hypersélective le contenu des communications sans compromettre leur sécurité. Ce n'est pas une position politique ou un parti pris : c'est une question scientifique. Celle-ci n'est d'ailleurs pas nouvelle puisque les cryptologues s'y intéressaient avant qu'elle devienne un sujet sociétal important. Personne n'a apporté de solution à ce problème dans une conférence publique.

Je vais essayer d'expliquer de façon compréhensible pourquoi nous considérons qu'un accès sélectif à certaines conversations affaiblirait le chiffrement de manière massive. Il est déjà relativement complexe de développer un système sans faille. Il peut paraître simple d'envoyer un message d'un point A à un point B. Tel n'est pas le cas, et nous avons beaucoup souffert pour y parvenir. La contrainte supplémentaire que constituerait la possibilité d'ouvrir un message spécifique à un instant T dans le futur rend impossible le maintien du même niveau de sécurité. Elle affaiblirait donc nécessairement la sécurité de l'application.

M. Benjamin Beurdouche. Cette possibilité d'ouvrir un message implique de casser une propriété de sécurité bien particulière appelée *forward secrecy* (confidentialité persistante). Les protocoles modernes protègent les anciens messages. Au fur et à mesure que l'on consomme le déchiffrement des messages reçus, les anciens messages sont protégés et ne sont plus déchiffrables. L'ouverture d'un message de manière sélective casserait la propriété de sécurité empêchant l'ouverture des messages antérieurs. Nous nous trouvons donc dans une impasse technique de base. C'est donc impossible.

En revanche, tout le monde est d'accord pour dire que l'accès légitime, mandaté par la justice, à des téléphones ou à des systèmes d'information pour lutter contre le crime organisé ou favoriser le renseignement, doit être effectif dans une démocratie. Les moyens pour le faire, qui permettent de contourner le chiffrement ou d'attaquer directement les terminaux, existent déjà et sont réglementés par la loi. Ils ne sont peut-être pas assez nombreux ni assez disponibles. Plutôt que de chercher à toucher à la sécurité globale du chiffrement, qui affaiblirait tout le monde, sans doute est-il donc préférable de favoriser l'utilisation des outils déjà existants, dans lesquels le ministère de l'intérieur a peut-être moins investi que le ministère des armées.

M. le président Philippe Latombe. Une messagerie soumise à un dispositif équivalent à celui que prévoyait l'article 8 *ter* verrait-elle la confiance des utilisateurs et sa capacité à se développer entamées ? Signal avait dit que, en cas d'adoption définitive de l'article, elle ne serait plus disponible en France. Quel risque représente un tel dispositif pour une entreprise comme la vôtre ?

M. Matthieu Finiasz. Si Olvid annonçait la mise en place d'un système permettant d'ouvrir les messages sur demande de la justice, nous perdrions des utilisateurs. Les forces de l'ordre ont besoin à la fois de garantir la protection de leurs communications et de pouvoir accéder à des informations sur des actions criminelles. C'est donc compliqué pour elles, car les outils qu'elles utilisent peuvent être aussi utilisés par des personnes malveillantes. Je pense que les utilisateurs des ministères, auxquels la directive Borne a imposé l'utilisation d'Olvid, s'arrêteraient d'utiliser notre système du jour au lendemain. Nous perdrions également nos certifications Anssi qui ne se sont accordées qu'à des applications protégées par de la bonne cryptographie. Cela aurait donc pour nous un énorme impact, d'autant plus que notre but n'est pas d'aller chercher des marchés hors de France. Notre application peut être utilisée partout dans le monde, mais nous avons créé cette société pour pouvoir protéger les communications des administrations et des entreprises françaises, car il y avait un manque en Europe et en France d'une messagerie avec notre modèle de sécurité.

M. Thomas Baignères. Nous aurions dû mettre la clé cryptographique sous la porte. Nous perdrions en effet notre avantage – une garantie cryptographique mathématique de sécurité – par rapport à celui d'autres solutions, comme Signal ou d'autres, qui repose davantage sur leur infrastructure. Nous ne nous contentons en effet pas de chiffrement de bout en bout puisque nous y ajoutons l'authentification de bout en bout. Notre sécurité ne dépend pas d'un serveur qui distribue des clés. Notre modèle de sécurité a mis la barre plus haut par rapport à de nombreuses autres messageries grand public au niveau mondial. Une solution *backdoor* intégrée à Olvid nous ferait perdre tout avantage concurrentiel.

Je n'aime pas l'approche qui consiste à menacer de quitter la France. D'ailleurs, si d'autres pays décidaient de voter le même genre de loi, la messagerie ne serait plus utilisée par personne. Nous préférons discuter et expliquer les choses, comme nous le faisons aujourd'hui et continuerons à le faire.

M. Benjamin Beurdouche. Ce ne seraient pas seulement les utilisateurs de l'administration qui quitteraient l'application, mais aussi ceux de la criminalité organisée. Il faut prendre en compte l'ensemble de l'écosystème. Même si la criminalité organisée – ou les services de renseignement étrangers – utilise ses propres clients, comme EncroChat, elle a recours également aux messageries grand public.

Mme Anne Le Hénanff, rapporteure. Nous avons la possibilité de supprimer l'article 16 *bis* du projet de loi. Êtes-vous prêts à discuter pour trouver des solutions ou demandez-vous impérativement de le maintenir ?

M. Matthieu Finiasz. Cela fait des années que nous vivons sans une telle disposition et nous arrivons à nous en sortir, mais le maintenir serait une très bonne chose. Il s'agirait, non pas de gêner les forces de l'ordre, mais d'exprimer une position forte de l'Assemblée nationale en faveur de la protection des données personnelles de la population. Nous pourrons survivre sans, nous n'en avons pas un besoin impérieux, mais il nous rassurerait contre le retour éventuel d'un article 8 *ter*.

M. Benjamin Beurdouche. Je ne suis pas très âgé, mais j'ai déjà vu revenir ce type de discussion plusieurs fois et, à chaque fois, nous devons refaire un effort scientifique d'explication. L'avis de la communauté scientifique n'a pas bougé d'un iota sur ce point depuis des décennies.

Personnellement, je préférerais que cet article soit maintenu, car il apporte un confort de sécurité, sans changer la vie des services de renseignement. Il n'empêche pas non plus la discussion et nous sommes totalement disponibles. Si, un jour, une proposition scientifique validée par la communauté permettait d'ouvrir les messages sans compromettre leur sécurité, il serait alors toujours possible de supprimer cette disposition.

M. le président Philippe Latombe. Je vous remercie.

14. Deuxième audition de M. Vincent Strubel, directeur général de l'ANSSI, mardi 15 juillet 2025 à 17 heures

Lors de sa réunion du mardi 15 juillet, la commission spéciale a procédé à une nouvelle audition, ouverte à la presse, de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI).

M. le président Philippe Latombe. L'audition – la dernière du cycle – des représentants de l'Agence nationale de la sécurité des systèmes d'information (Anssi), en particulier de son directeur général, vise à répondre aux questions qu'ont soulevées celles qui l'ont précédée.

M. Éric Bothorel, rapporteur général. Intercommunalités de France défend une trajectoire d'indépendance numérique européenne (TIE Break), pour que l'Anssi évalue les outils des collectivités et fasse des préconisations. Qu'en pensez-vous ?

La Martinique a subi une cyberattaque mais les techniciens n'ont pas pu rester sur place jusqu'à la fin du sinistre. Pourriez-vous rassurer nos collègues d'outre-mer ?

L'Anssi pourrait délivrer un label de conformité à la directive NIS 2. Y êtes-vous favorable ?

La mise à jour de votre référentiel gagnerait-elle à se faire en concertation avec les organisations professionnelles de la filière cyber française ? Faut-il intégrer ce référentiel dans la loi ? Plusieurs acteurs s'inquiètent d'être renvoyés à un trop grand nombre de décrets. Le législateur doit-il détailler la transposition de NIS 2 ?

La nouvelle revue nationale stratégique (RNS) a été publiée hier. Son quatrième objectif est d'atteindre une résilience cyber de premier rang. Quelles sont les implications pour l'Anssi ? Le projet de loi va-t-il assez loin en la matière ?

La RNS prévoit « des financements d'amorçage au profit des secteurs et des acteurs les plus vulnérables » ainsi que le renforcement des centres de réponse aux incidents de sécurité informatique (CSIRT). Vos orientations budgétaires en tiennent-elles compte ?

M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information. Le chiffrement est un problème complexe, que le projet de loi ne suffira pas à résoudre. Mon point de vue n'est pas politique – vous entendrez par ailleurs celui de la ministre déléguée Clara Chappaz. Comme l'a dit mon chef, le secrétaire général de la défense et de la sécurité nationale (SGDSN), il faut du temps pour expertiser les différentes options, dont aucune n'est pleinement satisfaisante. Il appartiendra ensuite au législateur de choisir.

En qualité de représentant de l'Anssi, je peux difficilement me prononcer contre l'article 16 *bis*. Toutefois, ce dernier visait à répondre à l'article 8 *ter* de la proposition de loi « narcotrafic », supprimé au cours de la navette. Il n'est peut-être pas nécessaire de le conserver.

La RNS prévoit de maintenir une cyber-résilience de premier rang. En matière de cybersécurité, grâce aux moyens dont dispose l'Anssi et à son organisation adéquate, la France n'a pas à rougir de son positionnement. Toutefois, nous sommes à un moment de bascule ; il faut redoubler d'efforts pour conserver notre niveau. La transposition et la bonne application de NIS 2 constituent un chantier majeur.

Ce n'est pas le seul. Nous devons également travailler sur la formation pour créer le vivier de talents qui nous fait défaut. Il faut améliorer le Centre de coordination des crises cyber (C4) pour actionner tous les leviers possibles en cas d'attaque du haut du spectre – de niveau étatique. Dans le domaine international, nous devons continuer à développer des alliances car cela favorise la stabilité. Nous

devons enfin redoubler d'efforts dans le domaine de l'autonomie stratégique et de la maîtrise des technologies.

Évidemment, notre principal défi sera de développer la cybersécurité à très grande échelle, au-delà du cœur régalien et des entreprises les plus stratégiques, déjà bien protégées – même si elles ne peuvent s'endormir sur leurs lauriers. Il est donc normal que la transposition et l'application de NIS 2 figurent en bonne place dans la liste des objectifs stratégiques, pour répondre à une menace de plus en plus massive. Le texte issu du Sénat prévoit d'ailleurs une stratégie nationale en matière de cybersécurité, conformément à la directive. Tout cela, qui forme le cœur de la réponse de l'État, sera précisé dans les prochains mois – il ne m'appartient pas d'en définir le calendrier.

Des financements seront nécessaires. En la matière, il revient au premier ministre de donner les orientations. La revue nationale stratégique exprime le souhait de pérenniser les CSIRT, en suivant plutôt une logique de cofinancement. Ils sont devenus des relais : dans un champ connexe à celui de l'Anssi, ils apportent aux victimes une aide précieuse. Parfois, ils choisissent de s'intégrer aux dispositifs d'accompagnement que les régions déploient en faveur du développement économique, en gardant une liberté d'organisation et de positionnement. Ce sont donc des acteurs importants de l'élargissement que nous appelons tous de nos vœux.

Vous nous interrogez sur l'opportunité de nous concerter avec les acteurs de la filière pour mettre à jour le référentiel de mesures. C'est notre souhait ; d'ailleurs nous agissons en ce sens depuis le début. La première version a été communiquée aux fédérations professionnelles représentant les assujettis et les futurs assujettis à NIS 2 – ceux du domaine privé ainsi que les associations d'élus représentant les collectivités territoriales. Depuis, nous leur avons transmis une nouvelle version qui prend en compte leurs retours. Tout l'écosystème a intérêt à y travailler ensemble, afin que chacun comprenne les mesures : les destinataires comme ceux qui les accompagneront pour les mettre en œuvre.

L'Anssi doit relever un autre défi dans le défi : il faut placer la barre à la juste hauteur. Si le niveau d'exigence est trop élevé par rapport à la maturité des entités concernées, celles-ci, confrontées à des exigences contradictoires et à des obstacles insurmontables, n'amélioreront pas leur cybersécurité. Si nous plaçons la barre trop bas, elles seront contraintes de prendre des mesures qui auront un coût mais pas d'efficacité. Nous y travaillons donc étroitement avec les acteurs de l'écosystème.

De manière générale, dans un domaine aussi mouvant que le numérique, il vaut mieux éviter d'inscrire dans la loi des mesures techniques car cela empêche de les actualiser au rythme de l'évolution générale. S'agissant du référentiel en particulier, cela nous priverait des avantages du dialogue avec les fournisseurs de solutions et avec les assujettis. Or nous aurons besoin de le préciser et de le corriger, grâce aux retours d'expérience du début de l'application de NIS 2 – la copie initiale comportera sûrement des erreurs. Nous serions par ailleurs empêchés de poursuivre

l'indispensable travail d'harmonisation avec les autres États membres et avec la Commission européenne. En effet, même si l'application ne sera pas strictement équivalente dans tous les pays – ce n'est pas un règlement –, il conviendra de gommer les difficultés de mise en œuvre transfrontalière. Pour toutes ces raisons, il est nécessaire d'en rester au niveau réglementaire ou infraréglementaire.

Le Sénat a prévu que l'Anssi pourrait approuver un label de confiance attestant la conformité à NIS 2. Il serait délivré aux entités assujetties, qui pourraient par exemple s'en prévaloir auprès des assureurs. L'idée nous intéresse. Des amendements rédactionnels seront peut-être nécessaires pour assurer la sécurité juridique du dispositif. Pour le reste, l'équilibre trouvé au Sénat est le bon : il faut un moyen de garantir la conformité, non une exigence de conformité. Imposer la labellisation à tous serait excessif.

Je précise que les fournisseurs de solutions numériques et les prestataires de services ne sont pas concernés. Des labels spécifiques existent déjà. L'Anssi délivre des qualifications et un label ExpertCyber. Un travail a été engagé pour les faire converger et pour les adapter aux exigences de la directive. J'y crois davantage qu'à la création d'un label supplémentaire dans un système déjà complexe : aucun de ceux qui existent n'est superflu mais il n'est pas besoin d'en ajouter. Avec le groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma), nous travaillons à intégrer le rôle des experts cyber dans le dispositif d'accompagnement à l'application de NIS 2.

Vous avez raison, l'Anssi est intervenue en 2023 pour la collectivité territoriale unique (CTU) de Martinique, qui avait subi une attaque par rançongiciel. Toute paralysie d'une collectivité est dramatique mais c'est particulièrement vrai des collectivités uniques car de nombreuses missions de service public essentielles sont touchées. L'Anssi a donc dépêché une équipe. Nous le faisons rarement : le plus souvent, les experts travaillent mieux en restant à leur poste, où tous les outils sont à leur disposition. Dans ce cas, l'équipe a gagné du temps sur la phase initiale de diagnostic en allant sur place, où elle a pu prendre tous les contacts nécessaires et établir un état des lieux. Ensuite, elle est rentrée dans nos locaux à Paris, non parce qu'elle avait renoncé à assister la victime, mais parce qu'elle y était plus efficace.

Je veille particulièrement à réserver le meilleur traitement possible aux cyberattaques affectant les services publics des territoires d'outre-mer – d'autres ont aussi reçu des équipes dans ce cadre. En effet, les conséquences sont beaucoup plus vite dramatiques en cas d'insularité : on ne peut les modérer en recourant à une substitution de service d'un voisinage proche ou à un plan blanc. Toutefois, le déplacement a pour seul objectif de poser un diagnostic ; nos agents effectuent le travail de remédiation depuis nos locaux, en lien avec les équipes sur place.

Votre première question concernait les technologies des collectivités. Sans me prononcer sur une initiative en particulier, je confirme que nous avons intérêt à travailler avec elles sur les solutions qu'elles déploient. Dans le domaine du

numérique en général, à plus forte raison dans celui de la cybersécurité, les difficultés vont croissant. Pour les surmonter, nous avons donc également intérêt à encourager, sans les forcer, les logiques naturelles de mutualisation des efforts. C'est pour cette raison que la transposition de NIS 2 concerne les intercommunalités plutôt que les communes – à l'exception des plus grosses. Certains acteurs ne peuvent entrer dans le périmètre du texte, comme les opérateurs publics de services numériques (OPSN), dont les statuts sont variés. Ils participent néanmoins à la mutualisation. L'Anssi travaille déjà avec eux, elle continuera *a fortiori* dans le cadre de l'application de NIS 2.

Mme Anne Le Hénanff, rapporteure. Vous avez évoqué les possibles différences de transposition. Elles risquent de poser des difficultés aux entreprises qui possèdent des filiales dans d'autres États membres. Le projet de loi peut-il les résoudre ?

Certaines dispositions devront être précisées par décret, en particulier concernant le référentiel prévu à l'article 14 ; les entreprises, notamment, s'en inquiètent. Sommes-nous allés assez loin dans ce domaine ? Pouvez-vous garantir que les décrets seront pris suffisamment tôt après la promulgation de la loi d'une part, qu'ils seront élaborés en concertation avec toutes les parties prenantes d'autre part ?

D'autres inquiétudes concernent l'indépendance des organismes qui effectueront les contrôles. Le projet de loi doit-il exclure certains acteurs ?

La loi s'appliquera-t-elle aux sous-traitants des principales entités concernées ? Seront-ils en mesure d'en respecter les exigences ?

Après la promulgation de la loi, la question se posera des compétences respectives des CSIRT et du GIP Acyma ainsi que de leur articulation. À ce jour, la réponse n'est pas claire. Le texte mentionne les premiers, dont l'avenir financier est incertain, mais non le second.

M. Vincent Strubel. S'agissant d'abord de la directive REC (directive du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques), nous avons collectivement choisi ce type d'acte normatif, car il nous semblait déraisonnable de procéder à une harmonisation maximale à l'échelle de l'Union européenne. Sa transposition est donc par définition différente d'un État membre à l'autre.

Par ailleurs, concernant l'articulation entre le siège et les filiales, tout n'est pas flou, la directive établissant qu'une entité juridique est soumise au cadre juridique établi par l'État membre dans lequel elle est présente. Il n'y a pas d'ambiguïté sur ce point.

En revanche, je reconnais qu'il y en a une au sujet de la soumission, ou non, aux différents seuils, selon lesquels une société est considérée comme une entité importante ou essentielle. Une certaine souplesse demeure – ce qui est peut-être une

bonne chose – quant au regroupement, ou non, des différentes filiales au sein d'un même groupe. Nous poursuivons le dialogue avec les États membres et la Commission européenne sur ce point, afin d'éventuellement apporter des éclaircissements, ce qui pourrait être bénéfique, sans toutefois, j'y insiste, chercher à tout rigidifier.

Il convient en effet de conserver une liberté de choix concernant les différentes entités. Je ne vois pas d'inconvénient à ce qu'un groupe choisisse d'uniformiser son traitement et de déclarer que toutes ses filiales sont assujetties au même statut et aux mêmes règles ou, au contraire, opte pour un traitement différencié, en fonction de l'activité des entités. Imposer une solution unique se ferait nécessairement au détriment des acteurs car, selon les situations, il est plus intelligent d'uniformiser ou de spécialiser.

Cela me conduit à votre question suivante : oui, l'équilibre entre la loi et le décret est le bon. Là aussi, nous aurons des éclaircissements à mesure que la Commission nous en apportera et que nous appliquerons la directive. En effet, comme je l'ai dit, il ne faudra pas moins de trois ans, une fois que le cadre sera posé, pour que nous vérifiions la conformité complète à la directive. C'est pourquoi j'estime qu'il faut conserver cette souplesse entre les dispositions législatives et réglementaires, voire infraréglementaires. Je suis conscient que ne pas avoir un texte législatif unique regroupant l'ensemble des critères, y compris techniques, est source de frustration chez certains acteurs, mais je pense que c'est le bon équilibre.

Je précise à cet égard que l'ajout, par le Sénat, de certaines définitions dans la loi contribue à ce bon équilibre, car il ne s'agissait pas d'éléments particulièrement techniques. Cela étant, je ne crois pas qu'il faille faire de même d'autres aspects, qui ont vocation à figurer dans les décrets.

Quant au fait que ces derniers soient élaborés tôt et de manière concertée, j'y suis naturellement favorable. Les décrets seront, *in fine*, pris par le premier ministre, aussi n'ai-je pas à me prononcer en son nom, mais la concertation avec tous les acteurs est engagée depuis septembre 2023 concernant le projet de loi et elle a depuis été étendue aux futurs textes réglementaires. Il y a des choses que nous ne pourrons pas faire avant que la loi soit adoptée, car les décrets ne feront que décliner ses dispositions, mais je répète que nous avons commencé à échanger avec plus de soixante-dix fédérations professionnelles et l'ensemble des associations d'élus, car c'est bien dans notre intérêt que d'avoir quelque chose de compréhensible, qui place la barre au bon niveau et qui soit de nature à être appliqué rapidement par l'ensemble de l'écosystème. Le travail est appelé à se poursuivre et, comme je l'ai dit, je suis attaché à ce que le cadre législatif et réglementaire soit fixé le plus vite possible, puis que nous laissions passer au moins trois années – temps nécessaire et incompressible – avant d'exiger une conformité complète.

S'agissant ensuite des audits de sécurité, la loi prévoit que l'Anssi peut recourir à des organismes compétents pour les mener ou y participer. Dans les deux cas, l'établissement de la liste des organismes habilités nous revient et nous serons

vigilants pour ne pas nous exposer à des risques de compromission ou d'ingérence étrangère. Je ne suis donc pas certain qu'il faille définir les règles de recours à des auditeurs au niveau législatif, sachant que le code de la défense prévoit déjà un cadre – mais il serait malvenu de ma part de m'opposer à ce que ce soit le cas si cela devait être jugé nécessaire. L'Anssi recourt à des prestataires qualifiés qui apportent l'ensemble des garanties nécessaires. Même si des inquiétudes légitimes peuvent être soulevées, je crois que nous saurons y répondre. En quelque sorte, nous ne jouerons pas contre notre propre camp.

Pour ce qui est des sous-traitants, ils ne sont pas directement soumis aux exigences de la directive NIS 2. Y remédier serait une surtransposition, ce que je ne pense pas souhaitable. En revanche, ils seront inclus dans le référentiel de mesures, dont nous avons partagé la version intermédiaire avec les futures entités concernées.

D'abord, il faut dans tous les cas établir une cartographie des sous-traitants numériques. Cette recommandation se fonde sur notre expérience. Quand nous intervenons en tant que pompiers, nous nous retrouvons souvent face à des assaillants qui comprennent mieux l'environnement de la victime que la victime elle-même, car elle ne dispose pas de la cartographie de ses sous-traitants. Or quand on doit tout reconstruire, on part avec un sacré handicap ! Conserver une traçabilité fera donc partie des exigences, d'autant que ce n'est pas un élément très complexe.

Ensuite, répercuter les exigences applicables aux sous-traitants par voie contractuelle coule de sens. Cela ne s'écrit d'ailleurs pas de manière très détaillée, car les choses dépendent fortement de la nature des sous-traitants.

Enfin, si les sous-traitants ne sont pas intrinsèquement soumis à la directive, les acteurs du numérique, eux, le sont et font l'objet d'un acte d'exécution harmonisé à l'échelle européenne, qui, sauf erreur, a été pris en octobre dernier par la Commission. Ainsi, les sous-traitants numériques seront directement régulés en tant qu'entités importantes ou essentielles. Quant aux autres, les relations seront d'ordre contractuel et une traçabilité s'impose.

J'en viens à votre dernière question, qui n'est pas la moins importante : l'équilibre entre les CSIRT et le GIP Acyma. Ils ne sont pas redondants, mais complémentaires. Le GIP, que j'ai l'honneur de présider, ne répond pas lui-même aux incidents ; il en serait d'ailleurs bien incapable compte tenu de ses moyens. Il oriente les victimes de cybermalveillance vers les acteurs susceptibles de les aider par l'intermédiaire de la plateforme cybermalveillance.gouv.fr. Au total, 1 200 prestataires privés sont référencés, parmi lesquels 200 sont labellisés comme experts cyber, et depuis le 17 décembre dernier, un renvoi vers les forces de sécurité intérieure – police ou gendarmerie – est possible au travers du service 17Cyber, par exemple pour instruire un pré-dépôt de plainte.

Demain, en vertu des travaux financés par l'Anssi et lancés conjointement avec le GIP, les CSIRT territoriaux feront partie des répondants. Leur métier est de traiter les incidents, de coordonner la réponse, voire de renvoyer vers des

prestataires privés, mais en concertation avec les victimes, ce que ne peut pas faire le GIP Acyma.

Ainsi, le GIP est appelé à répondre aux actes de cybermalveillance et la plateforme 17Cyber à remplacer progressivement le site cybermalveillance.gouv.fr afin d'avoir une signalétique simple. Selon leurs choix et leurs besoins, les victimes seront orientées vers les prestataires privés, les CSIRT s'ils sont adaptés à leur cas, ou les forces de l'ordre. Au fond, un guichet unique renverra vers les bons répondants. Le fonctionnement sera donc comparable à celui du Samu qui, selon les cas, envoie un véhicule de secours, oriente vers la médecine de ville, engage à se rendre aux urgences par ses propres moyens, etc. Avoir une plateforme de référence renvoyant vers la réponse adaptée est selon moi la bonne approche, car les besoins sont très variables suivant la nature de l'attaque.

Je précise que la mission du GIP Acyma ne se résume pas à la réception des actes de cybermalveillance et inclut un important travail de prévention. L'organisme accomplit d'ailleurs une action formidable en la matière en sensibilisant à grande échelle, ce qu'il est le seul à faire au niveau national en ce qui concerne les particuliers et les petites structures. C'est un rôle essentiel qu'il continuera de jouer.

Quant au financement des CSIRT, l'objectif est de trouver un modèle de cofinancement au sein de la revue nationale stratégique, ce qui renvoie aux débats budgétaires sur lesquels je ne suis pas légitime à m'exprimer.

M. Mickaël Bouloux, rapporteur. J'aurai deux questions concernant le titre III du projet de loi, qui transpose le règlement Dora (règlement sur la résilience opérationnelle numérique du secteur financier).

La première a trait à un sujet régulièrement soulevé lors de nos auditions : les relations entre les entités financières et leurs prestataires de services en technologies de l'information et de la communication (TIC). Vous le savez, le règlement Dora prévoit des obligations plus strictes en matière de contractualisation, afin de se conformer au nouveau cadre de gestion des risques liés à l'utilisation des TIC. Dès lors, les prestataires pourraient se voir soumis à des audits. Cependant, ce faisant, ces derniers ne seront-ils pas amenés à communiquer des données sensibles, voire à devoir se soumettre à des enquêtes intrusives de la part de cabinets étrangers, quand bien même ils agiraient pour le compte d'entités financières françaises ? Il revient au législateur de réfléchir aux moyens d'éviter toute ingérence économique étrangère, en trouvant un dispositif comparable à la loi dite de blocage de 1968, ou encore en confiant à une autorité tierce l'arbitrage entre les demandes des cabinets d'audit et les objections des entreprises contrôlées. Qu'en pensez-vous ? Partagez-vous ces inquiétudes ou estimez-vous que nos entreprises sont suffisamment à l'abri de ce type d'intrusion ? La présidente de l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse) nous a suggéré de vous interroger sur cette question.

Quant à ma seconde question, elle porte sur le délai d'application des dispositions du titre III pour les sociétés de financement. Le texte issu du Sénat prévoit que les mesures liées aux exigences prudentielles spécifiques aux prestataires de services bancaires – dont font partie les sociétés de financement – n'entreront en vigueur qu'au 1er janvier 2030, quelle que soit la taille des sociétés. De plus, les sénateurs ont retenu un principe de proportionnalité s'agissant de l'application des mesures par les sociétés de financement les plus petites. Quelle est votre opinion ? Une application tardive du projet de loi pour les sociétés de financement présente-t-elle des risques ?

M. Vincent Strubel. Auditer un système d'information ou plus généralement une entreprise n'est pas une opération à exécuter à la légère. C'est pour cette raison que la définition de la liste des prestataires demeure, aux termes du titre II, à la main de l'Anssi et que nous avons établi, en 2014, une qualification spécifique pour les prestataires d'audit de la sécurité des systèmes d'information – le référentiel Passi –, qui atteste de la compétence technique des sociétés et des garanties qu'elles présentent pour protéger les données, voire les détruire à l'issue de l'audit.

Je ne me risquerai pas à émettre des préconisations dans un champ qui relève plutôt de l'Autorité de contrôle prudentiel et de résolution (ACPR) et de la Banque de France, mais il serait de bon aloi de prévoir un encadrement ou des recommandations. À l'instar de ce que prévoit la directive NIS 2, il ne s'agit pas nécessairement de définir dans la loi un référentiel pour les prestations d'audit, mais de prévoir l'établissement d'une liste de prestataires approuvés par une autorité indépendante.

Quant aux délais d'application, je ne m'avancerai pas sur le cas spécifique des sociétés de financement, mais la question se pose aussi s'agissant des mesures prévues au titre II du projet de loi. La menace cyber est en augmentation et préexistait même à l'élaboration de la directive NIS 2. Ainsi, plus on attend et plus il y aura de victimes. Pour autant, je suis bien placé pour savoir que répondre à cette menace et se mettre en conformité avec la directive NIS 2 et le règlement Dora demandent du temps. Le contrôle de conformité avec les actes européens n'aura lieu que trois ans après l'établissement du cadre national complet, c'est-à-dire des lois et décrets.

Il est délicat de se prononcer sur un délai raisonnable s'agissant du secteur financier. Je laisse aux acteurs qui le connaissent mieux que moi le soin de s'exprimer sur l'horizon 2030 fixé par le Sénat.

Mme Catherine Hervieu, rapporteure. L'Anssi a vu son budget baisser cette année de 3,5 millions d'euros. L'établissement avait pourtant demandé 35 millions d'euros de crédits hors salaires et la création de soixante emplois afin de conduire la réforme que nous évoquons aujourd'hui. Maintenez-vous ces demandes budgétaires et en personnels pour l'année prochaine afin de mener à bien les missions qui vous sont confiées et l'approfondissement prévu par le projet de

loi ? J'ai bien compris que vous n'étiez pas présent aujourd'hui pour aborder ce sujet, mais la question des moyens ne saurait être éludée.

Par ailleurs, la résilience numérique dépend aussi de la formation et des compétences. En Ukraine, par exemple, la cyberadministration est très avancée. Quelle devrait être l'implication de la société civile et pourrait-elle devenir un outil asymétrique redoutable ?

À cet égard, que pensez-vous de la création d'un module de formation destiné aux élus locaux ? Vous avez dit souhaiter placer la barre au bon niveau. Il faut que le texte que nous examinerons en septembre soit cohérent avec la proposition de loi portant création du statut de l'élu local, que nous venons d'adopter.

M. Vincent Strubel. Concernant le budget de l'Anssi, non, le besoin n'a pas changé, mais il faut le confronter à la situation financière que nous connaissons tous. Comme l'ensemble des administrations, l'agence connaît une année 2025 particulièrement contrainte et il n'y a pas de raison pour qu'elle bénéficie d'un traitement de faveur. La revue nationale stratégique remet les enjeux de sécurité et de défense, ainsi que les besoins qui les sous-tendent, sur le devant de la scène et s'intégrera dans les débats budgétaires éminemment complexes sur lesquels je ne m'avancerai pas.

De fait, l'application de la directive NIS 2 requiert la création de 50 à 60 équivalents temps plein (ETP) : c'est le nerf de la guerre pour que l'Anssi puisse assurer ses missions de supervision et de contrôle. Même si nous ne sommes pas dans une logique punitive, sans contrôleurs, toutes les préconisations légales resteraient sans effet et notre crédibilité serait amoindrie. De même, nous avons besoin de personnels pour renforcer notre accompagnement des différents secteurs et territoires. Notre objectif n'est pas de faire les choses à la place des acteurs de terrain, mais de travailler efficacement avec eux de manière complémentaire. Cela fait écho aux échanges que nous venons d'avoir au sujet des CSIRT. Ainsi, ce n'est donc pas tant pour ses propres activités que l'Anssi a besoin de crédits, mais pour financer les différents dispositifs d'accompagnement.

S'agissant des compétences, il s'agit du point le plus essentiel de la transposition et de l'application de la directive NIS 2 et plus généralement de notre plus grand défi. Actuellement, le facteur qui limite le plus nos ambitions en matière de cybersécurité est notre capacité à trouver des personnes formées. On parle de 40 000 voire 60 000 personnels manquants dans ce domaine. L'Anssi agit pour y remédier, mais il faut changer d'échelle. Nous travaillons depuis longtemps avec les formations supérieures aux niveaux BTS (brevet de technicien supérieur), licence et master, mais celles-ci ne font pas le plein, ce qui signifie que nous n'attirons pas suffisamment de jeunes vers ces parcours. Avec le ministère de l'éducation, nous œuvrons pour que le service Pix intègre la cybersécurité dans les questionnaires proposés aux collégiens et aux lycéens, ou encore pour que le Campus cyber promeuve ce secteur auprès des plus jeunes et les attire vers ces

métiers formidables où on manque de monde. Enfin, des actions sont aussi engagées dans le domaine de la formation professionnelle, afin de permettre davantage de reconversions. C'est un enjeu clé de la cyber-résilience, évoqué dans le quatrième objectif stratégique de la revue nationale stratégique.

La formation ne se limite pas aux métiers de la cybersécurité. Former les élus, les décideurs est un enjeu fondamental. La bonne compréhension des enjeux de la cybersécurité et, plus généralement, du numérique est une des clés de la résilience de notre société face à une menace hybride qui ne va pas en s'amenuisant. Tout ce qui peut favoriser cette compréhension est bon à prendre ; je continuerai à y travailler. L'Anssi propose, depuis de nombreuses années, un Mooc (module de formation en ligne), qu'il nous faudra, si nos moyens nous le permettent, ajuster et faire évoluer pour diffuser des messages de sensibilisation à grande échelle.

Nous n'avons pas à rougir de notre capacité à mobiliser le secteur privé, surtout si nous nous comparons à nombre de nos homologues étrangers. Nous avons su construire une action efficace en la matière grâce à différents cadres de qualification, à des prestataires de services, à des solutions du secteur privé, à des labels comme ExpertCyber – qui n'émanent pas de l'Anssi mais qui sont très complémentaires de notre activité –, au travail mené avec les filières – qui se concrétise par exemple par les campus cyber et les comités stratégiques de filière… Nous avons, en ce domaine, une véritable équipe de France qui transcende la frontière entre le public et le privé. Cette réalité n'est pas nouvelle. Nous avons remporté, collectivement, la médaille d'or lors des Jeux olympiques et paralympiques. Nous avons passé un test grandeur nature de notre capacité à agir collectivement : le succès que nous avons obtenu a dépassé toutes les attentes. La mobilisation de la société civile, à tout le moins du secteur privé, est une réalité et un modèle que nous essayons de diffuser à l'échelle européenne en introduisant, dans le champ du Cybersecurity Act, une certification des prestataires de services en matière de cybersécurité et en insistant sur ce volet dans le cadre de la réserve de cybersécurité prévue par le règlement européen sur la cybersolidarité.

Mme Anne Le Hénanff, rapporteure. L'article 19 du projet de loi indique que les offices et les bureaux d'enregistrement sont responsables du traitement des données nécessaires à l'enregistrement des noms de domaine et tiennent des bases de données à jour. À cette fin, prévoit le texte, « ils mettent en place des procédures, accessibles au public permettant de vérifier ces données lors de leur collecte […]. » La mention « lors de leur collecte » constitue, aux yeux de l'Afnic (Association française pour le nommage internet en coopération), une surtransposition. Qu'en pensez-vous ?

L'article 20 impose de conserver les données précitées pendant un an alors que, semble-t-il, les offices et les bureaux les conservent déjà pendant une durée bien supérieure. Pourquoi avoir ajouté cet article ?

Les représentants du secteur de la santé nous ont dit que les établissements de santé et médico-sociaux ne sont pas explicitement inclus dans le périmètre du projet de loi. Que leur répondez-vous ?

Les articles 38, 41 et 42 figurent dans le titre II bien qu'ils ne transposent pas NIS 2. Ils traitent respectivement de l'allègement de la procédure d'exportation des biens de cryptologie, du renforcement des sanctions pénales dans l'objectif d'améliorer la lutte contre les brouillages et du renforcement des conditions d'accès à une assignation de fréquence. Pourquoi figurent-ils dans le projet de loi ?

M. Éric Bothorel, rapporteur général. Je voudrais vous faire part de plusieurs préoccupations exprimées par CyberCercle et d'autres organismes.

La première concerne l'exclusion des ministères des étapes clés du processus de la transposition de NIS 2, contrairement à ce qui s'est fait pour REC et Dora.

La deuxième concerne les audits effectués par l'organisme indépendant mentionné à l'article 29. On nous a dit que le texte instaurait une inégalité de traitement, dans la mesure où il prévoit que certains contrôles seront à la charge des entités et d'autres, à celle de l'Anssi.

La troisième préoccupation porte sur le fait que l'article 37 ne prévoit pas de sanctions à l'encontre des administrations et des collectivités territoriales.

Le dernier motif d'inquiétude dont il nous a été fait part concerne l'incohérence entre les dispositifs de partage de l'information prévus par Dora et NIS 2. On nous a suggéré de transposer l'article 29 de NIS 2 pour éviter des inégalités entre entités.

Par ailleurs, le point 509 de la revue nationale stratégique indique qu'un « filtre de cybersécurité à destination du grand public visant à prévenir l'accès aux sites web malveillants sera déployé dès 2025 ». Cette mesure sera-t-elle réellement appliquée cette année ?

Enfin, le point 479 de la RNS énonce que « L'intérêt d'un véhicule législatif plus général sera examiné pour porter des mesures renforçant la résilience de la Nation […] dans le nouveau contexte géostratégique (politique de stockage stratégique […]) ». Est-il question d'avoir un nouveau texte et, le cas échéant, à quel horizon ?

M. Vincent Strubel. La question du stockage stratégique renvoie plutôt à la directive REC. La question de savoir s'il faut imposer la création de stocks stratégiques est toujours débattue.

Nous sommes toutes et tous convaincus de l'intérêt du filtre anti-arnaque que la RNS réaffirme. Je ne me prononcerai pas sur la question de savoir quelle est l'autorité la plus légitime pour le mettre en œuvre car cela relève des débats

interministériels, au sens large. Le GIP Acyma fait partie des acteurs qui pourraient jouer ce rôle. La loi définit les signalements qui pourraient donner lieu à un blocage – cela concerne plutôt des autorités administratives.

Le règlement Dora contient des règles particulièrement complexes concernant les données financières. Je ne porterai pas d'avis sur cette strate normative supplémentaire.

Le choix a été fait de ne pas étendre aux collectivités la logique des sanctions financières, qui s'appliquent uniquement au secteur privé. La ministre saurait, mieux que moi, expliquer ce choix politique. En tout état de cause, une collectivité ne fonctionne pas comme une entreprise, ne fournit pas le même service, n'est pas pilotée selon la même logique. Une sanction financière, qui est très opérante pour un acteur privé, l'est moins pour une collectivité ; elle s'applique au détriment des usagers et des missions de service public. Les moyens les plus efficaces à l'égard d'une collectivité résident dans les mesures d'exécution, notamment dans la possibilité de rendre publique une injonction. Cela revient à mettre un élu face à ses responsabilités en rendant public le fait qu'il ne respecte pas les mesures élémentaires de sécurité prescrites par la loi.

S'agissant de la prise en charge des contrôles, le point d'équilibre le plus naturel consiste à revenir aux dispositions de la directive, qui distingue les audits spécifiques, mis à la charge des entités contrôlées, et les contrôles plus génériques. Lorsque l'Anssi effectuera elle-même l'audit, celui-ci ne sera pas à la charge de l'entité ; il en ira autrement en cas de recours à des prestations spécifiques, comme des audits complémentaires. Le fait de mettre un contrôle à la charge de l'entité ne constitue pas une nouveauté. Le code de la défense prévoit déjà cette modalité pour les OIV (opérateurs d'importance vitale).

Les ministères n'ont pas exprimé le souhait d'endosser un rôle particulier dans le cadre de ce processus. Tout cela a fait l'objet, comme à l'accoutumée, d'une concertation interministérielle avant le dépôt du projet de loi. Le modèle qui a été choisi, et qui fait consensus, consiste à désigner une autorité centrale coordinatrice, comme y incite NIS 2. Cela se fera naturellement – conformément au fonctionnement normal de l'Anssi – en concertation avec les ministères. Cela étant, ces derniers jouent un rôle de coordination s'agissant des OIV, notamment pour leur désignation. Il s'agit là d'une compétence métier liée à chaque secteur d'activité. La directive NIS 2 ne prévoit pas de désignation individuelle des entités auxquelles elle s'applique : elle suit une logique de seuils conçue pour n'oublier personne. Des désignations individuelles sont toutefois prévues dans certains cas, qui nécessiteront l'expertise des ministères. Il n'y a pas lieu de prévoir, dans la loi, une compétence spécifique des ministères, qui n'aurait pas de sens eu égard à NIS 2.

Il serait en effet opportun que des corrections soient apportées à l'article 19. Nous vous proposerons un amendement à ce sujet.

Les établissements de santé seront soumis à la même logique de seuils que les autres acteurs. Il existe toutefois des cas limites qui appellent une désignation individuelle. Dans le domaine de la santé, en effet, la logique des seuils ne permettra pas nécessairement d'appréhender certains acteurs critiques. En concertation avec le ministère de la santé, voire avec les opérateurs, qui sont déjà, pour certains, des opérateurs de services essentiels au sens de la directive NIS 1, nous procéderons à la désignation individuelle d'acteurs. Cela étant, on n'assujettira pas la pharmacie du quartier : dans ce domaine comme dans d'autres, un seuil minimal doit être atteint, correspondant à la maturité ou à la taille de la structure.

Les dispositions relatives aux fréquences répondent à une demande de l'Agence nationale des fréquences (ANFR) ; leur présence dans le texte est assez légitime car il s'agit de la protection du spectre, qui s'inscrit aussi dans le champ de la directive.

L'article 38 propose – en écho à des demandes récurrentes des acteurs industriels – un allègement du régime de contrôle des exportations de prestations et de moyens de cryptologie, lequel avait été institué par la loi pour la confiance dans l'économie numérique de 2004. Ce texte, qui avait marqué l'aboutissement d'un long processus, avait libéralisé l'usage de la cryptographie tout en soumettant l'exportation à certains contrôles.

Deux régimes coexistent en matière d'exportation : un régime déclaratif et un régime d'autorisation, qui sont l'un et l'autre contrôlés par l'Anssi. Nous procédons, en cette matière, à une consultation interministérielle. Ces règles complexes donnent lieu à des récriminations légitimes de la part des acteurs qui souhaitent exporter des solutions numériques intégrant de la cryptographie – ce qui recouvre à peu près tout, à l'heure actuelle, dans le domaine numérique. Les critiques portent notamment sur le fait que le régime d'autorisation se superpose à un régime plus général, qui est celui du contrôle des biens à double usage : les entreprises doivent donc obtenir une double autorisation.

Le projet de loi propose, à titre de simplification, d'imposer un seul régime, de nature déclarative. Il est en effet nécessaire de recueillir des déclarations dans le domaine cryptographique pour comprendre les mécanismes et nourrir la capacité de l'Anssi à évaluer l'impact d'une vulnérabilité cryptographique. À titre d'exemple, lorsqu'un algorithme fondateur de la cryptographie fait l'objet d'une publication scientifique qui amenuise sa sécurité, il nous faut savoir dans quelles solutions il est déployé afin de coordonner très rapidement les efforts. En revanche, un régime d'autorisation n'a pas nécessairement d'utilité et est dans une certaine mesure redondant avec le contrôle des biens à double usage. L'Anssi appelle de ses vœux cette simplification, le double régime d'autorisation ayant perdu de son sens.

M. le président Philippe Latombe. Comme l'a montré le rapport d'enquête du Sénat sur les cabinets de conseil, la réalisation d'audits financiers ou technologiques peut permettre de capter des informations. Les cabinets ne mettent

pas toujours en pratique la muraille de Chine qui est souvent invoquée. Avez-vous des propositions de rédaction en ce domaine ?

Plus globalement, si vous avez des idées d'amendements à introduire dans le texte, n'hésitez pas à nous les communiquer le plus rapidement possible.

Pourriez-vous nous apporter des précisions sur la règle *non bis in idem* ?

Pouvez-vous vous engager sur la fréquence de publication – annuelle, bisannuelle, trisannuelle… – de la stratégie pluriannuelle de l'Anssi ?

Le choix de ne pas soumettre les collectivités à des sanctions financières répond certes à des considérations politiques, mais il faut aussi prendre en compte l'aspect juridique – le Conseil d'État s'est prononcé sur cette question dans son avis. Les collectivités nous ont dit que, faute de sanction, elles se sentiraient relativement libres d'agir à leur guise. Le RGPD (règlement général sur la protection des données), qui prévoit de telles sanctions pour les collectivités, n'a pas eu d'effet significatif sur leurs ressources. La question est de savoir si, le cas échéant, on rend passible de sanctions l'ensemble du secteur public, y compris les groupements hospitaliers de territoire (GHT), les GIP et les agences de l'État. On peut s'interroger sur la volonté d'un certain nombre de GHT de monter en compétences dans le domaine cyber. En outre, ne pensez-vous pas que le fait d'inclure dans le champ des sanctions des entités très sensibles, comme France Travail, serait un moyen de les faire progresser dans ce domaine ?

La norme ISO est-elle un référentiel suffisant ? Les éléments publiés par l'Enisa (Agence européenne de cybersécurité) prendront-ils le pas sur votre référentiel ?

Avez-vous une idée du montant de l'effort financier que représenterait le maintien des CSIRT ? Serait-il opportun d'autoriser leur cofinancement ?

Les dispositions de NIS 2, Dora et REC relèvent-elles du domaine régalien et, à ce titre, pourraient-elles relever de la responsabilité du futur État de la Nouvelle-Calédonie, si la réforme constitutionnelle allait à son terme ? Pouvez-vous prendre l'attache du ministère des outre-mer pour déterminer si l'on doit prévoir une disposition spécifique afin d'anticiper l'éventuelle validation de l'accord sur la Nouvelle-Calédonie ?

M. Vincent Strubel. S'agissant des cabinets d'audit, il est légitime de se préoccuper de la sécurité des données mais je ne pense pas que vous arriviez à traiter cette question globalement par le prisme étroit de l'encadrement des prestations d'audit en cybersécurité – lequel conserve, dans la plupart, des cas, un caractère non contraignant. Le référentiel Passi comprend plusieurs dizaines de pages éminemment techniques et prévoit des procédures de vérification assez lourdes. Des dispositions pourraient être insérées dans la loi au sujet d'autres domaines d'application de l'audit. Je demeure toutefois prudent concernant le domaine

financier, que je ne maîtrise pas dans ses ramifications métiers autres que la cybersécurité.

Le principe *non bis in idem* renvoie à l'articulation entre NIS 2 et le RGPD. Il est possible qu'à l'avenir, la Cnil (Commission nationale de l'informatique et des libertés) et la commission des sanctions instituée par le projet de loi pour réprimer les manquements à NIS 2 envisagent l'une et l'autre de sanctionner un même fait, qui constituerait à la fois un manquement au RGPD et à la directive. Le projet de loi prévoit que, dans ce cas, les sanctions financières ne pourraient être prises qu'au titre du RGPD, lequel fixe un quantum de peine double par rapport à celui de NIS 2. En revanche, les mesures d'exécution, les mises en demeure, qui sont décidées avant la sanction financière, peuvent se cumuler – du moins la loi ne l'exclut-elle pas. Cela étant, la coordination existante entre l'Anssi et la Cnil, dans le respect du statut de chacun, permet d'éviter que l'on se marche sur les pieds en cette matière. Si des mesures de contrôles, d'exécution, de pré-sanction financière étaient prises, elles feraient l'objet d'une coordination entre nos deux institutions.

Il est un cas qui ne figure pas dans la loi et qui n'a pas vocation à y être : c'est celui dans lequel une même entité fait l'objet de plusieurs procédures de sanction au titre de deux manquements distincts, l'un au RGPD, l'autre à NIS 2. Dans cette hypothèse, le principe *non bis in idem* ne s'applique évidemment pas. En revanche, la synchronisation des politiques de contrôle, qui existe de longue date, est amenée à se développer. Cela n'aurait pas grand sens, en effet, que la Cnil contrôle une entreprise et que l'Anssi fasse de même la semaine suivante. Nous pouvons travailler en bonne intelligence pour nous assurer que, dans le cadre des contrôles que nous menons, les critères d'appréciation soient similaires et qu'une forme de conseil soit apporté.

La mission de contrôle et de supervision placée au sein de l'Anssi, qui veillera, le cas échéant, à l'application de NIS 2, sera en lien étroit avec la Cnil comme avec d'autres autorités indépendantes. Nous avons besoin d'apprendre comment effectuer ce type de mission de contrôle – ce n'est pas inné pour l'Anssi. Il me paraît rassurant que ce ne soit pas une nouveauté pour la Cnil. En effet, celle-ci a l'habitude de se coordonner, par exemple avec la DGCCRF (direction générale de la concurrence, de la consommation et de la répression des fraudes), avec laquelle elle partage certains domaines de compétence.

M. le président Philippe Latombe. Pour que ce soit bien clair, un acte qui constituerait à la fois un manquement à NIS 2 et au RGPD ne fera pas l'objet de deux sanctions cumulatives ?

M. Vincent Strubel. Non.

M. le président Philippe Latombe. La sanction applicable en raison d'un manquement au RGPD serait-elle, dans ce cas de figure, majorée compte tenu du manquement simultané à NIS 2, ou la Cnil appliquerait-elle le même quantum de peine ?

M. Vincent Strubel. Dans cette hypothèse, la sanction serait prononcée au titre du RGPD sur le fondement du quantum de peine prévu par ce dernier. Le collège de la Cnil pourra décider souverainement de majorer la sanction, dans la limite prévue par le RGPD, en fonction de la gravité des faits.

M. le président Philippe Latombe. La plupart de vos homologues, dans les États européens, suivent-ils la logique du non-cumul des sanctions ? Certaines autorités pourraient-elles demander une majoration de la sanction pour manquement au RGPD au titre de la non-application de NIS 2 ?

M. Vincent Strubel. Une partie de la réponse dépend de la mise en œuvre des textes par chaque État membre : il faudra voir pour juger. Cela étant, le principe *non bis in idem* est, me semble-t-il, contenu dans la directive NIS 2, qui prévoit le cas de l'articulation avec le RGPD et la primauté de ce dernier en cas de manquement aux deux textes.

Vous m'interrogez sur la stratégie pluriannuelle. L'Anssi publie son propre plan stratégique – celui pour 2025-2027 a été mis à jour en mars. Quant à la stratégie en cybersécurité de la France, qui dépasse l'Anssi, elle paraîtra, avec le détail des mesures spécifiques, dans les prochaines semaines ou les prochains mois – il ne m'appartient pas de la révéler. On en retrouve les grandes orientations dans l'objectif stratégique 4 de la RNS. Le président de la République avait confié son élaboration au SGDSN et à un rapporteur qui n'est pas membre de l'Anssi : celle-ci y a été étroitement associée mais il est sain de bénéficier d'un regard extérieur. La fréquence de révision s'établirait sans doute à cinq ans. C'est raisonnable : le domaine est mouvant mais on ne peut établir une nouvelle stratégie tous les ans car cela nécessite une mobilisation intense de toutes les parties prenantes.

S'agissant des sanctions financières, la logique juridique tendrait à assujettir les collectivités au régime des entreprises privées. Il n'en va pas de même des administrations de l'État, qui dépendent du budget général. L'avis du Conseil d'État a bien été lu et entendu mais le choix, politique, a été fait de ne pas le suivre en la matière. D'autres sanctions et mesures d'exécution existent par ailleurs, en particulier la publication des manquements.

La norme ISO 27001 est un sujet aux multiples ramifications. Elle ne couvre pas tous les objectifs de NIS 2, seulement ceux relatifs à la gouvernance. Pour les entités importantes, deux objectifs de sécurité sur quinze sont concernés ; pour les entités essentielles, c'est deux sur vingt. En cumulant les exigences d'ISO 27001 et d'ISO 27002, qui la complète, le taux de couverture atteint 80 %. Les 20 % restants relèvent de la résilience et de la gestion de crise.

Le modèle belge requiert la conformité à ISO 27001 et le respect de mesures complémentaires issues de l'Institut national des normes et de la technologie (NIST) des États-Unis – d'autres normes internationales peuvent jouer le même rôle. Pour la France, nous souhaitons plutôt que soient d'abord définis des objectifs de sécurité puis que soient établies les normes afférentes. Je crois que les Allemands adoptent

la même démarche. Le référentiel listera les objectifs ; la conformité à ISO 27001 vaudra, par exemple, conformité aux objectifs 1 et 2, relatifs à la gouvernance ; la conformité à ISO 27002 à tel autre. En revanche, nous n'exigerons pas la conformité à ISO 27001, qui exige un travail intense : on pourra démontrer sa conformité autrement. En effet, ce n'est pas indispensable pour les entités importantes, qui ne pourraient pas toutes y parvenir – les concernant, l'exigence en matière de gouvernance sera sans doute inférieure à celle d'ISO 27001.

L'Agence européenne de cybersécurité (Aesri) a publié un guide d'exécution technique de NIS 2, non contraignant. Elle a ainsi contribué aux travaux menés, en France avec le concours de l'Anssi, pour clarifier les conditions d'application de la directive. Il faut néanmoins préciser que ce guide n'est applicable qu'aux acteurs du numérique, dont le traitement dépend de l'État d'implantation. Les autres acteurs relèvent de la transposition en droit national. Ses annexes dessinent les prémices d'une comparaison des différents référentiels nationaux. Cela confirme notamment que la norme ISO 27001 ne couvre pas tous les aspects. Nous allons poursuivre ce travail sur la déclinaison nationale dans les autres champs.

Combien coûtent les CSIRT ? En application du plan France relance, l'Anssi a versé à chacun 1 million d'euros pour trois ans. Il serait hâtif d'en déduire qu'un CSIRT coûte 333 333 euros par an. Ce fonds d'amorçage devait couvrir trois années de fonctionnement ; s'agissant d'une période d'incubation et de montée en puissance, elles ne sont pas forcément révélatrices.

Dès le départ, le choix a été fait de placer les CSIRT auprès des régions, qui pouvaient librement apprécier l'opportunité d'en créer un. Toutes ne l'ont pas fait. Le cas échéant, l'État, par l'intermédiaire de l'Anssi, soutenait l'initiative. Mieux vaut ne pas imposer un modèle unique assorti d'un financement intégral. L'échelon régional permet d'intégrer les CSIRT à la politique de développement économique, complémentaire de la politique régalienne de sécurité, qui relève de l'État. Les centres se trouvent ainsi à la croisée des deux chemins. Tout cela milite à la fois pour le cofinancement et pour une marge d'initiative locale.

Du point de vue de l'Anssi, il faut surtout que chaque CSIRT respecte un protocole standard. Plusieurs domaines, comme le traitement, la diffusion et la protection de l'information, doivent respecter des normes internationales. Nous pouvons ainsi parler à tous les CSIRT, sectoriels comme territoriaux, de la même manière. Si par ailleurs ils développent des activités annexes de conseil et d'accompagnement, s'ils adoptent des modèles de financement variables, tant mieux. Ils disposent ainsi d'un degré de liberté qui leur permet de mieux s'intégrer dans le contexte local. Certains, par exemple, s'adossent aux campus cyber territoriaux – c'est très bien. Il ne serait pas pour autant pertinent d'imposer à chaque région de créer son campus et de le financer pour que, à son tour, celui-ci contribue à financer un CSIRT. Il faut se laisser une marge de manœuvre.

Pour conclure sur ce point, la logique de cofinancement garantit que la démarche a un sens au niveau local. Toutefois, il ne faut pas laisser les régions assumer seules la charge des CSIRT, dont la mission est d'intérêt général. Il ne faut pas non plus trop cadrer les logiques de financement, tant qu'elles respectent la neutralité des centres.

M. René Pilato (LFI-NFP). Je suis d'accord avec vous, les mesures techniques n'ont pas à être inscrites dans la loi. Mais qu'en est-il des seuils relatifs au nombre de salariés et au chiffre d'affaires ?

Par ailleurs, vous disiez qu'il convenait d'établir une cartographie des sous-traitants numériques, ce qui est une excellente idée. Or il s'agit souvent de très petites entreprises, susceptibles de subir des actes de cybermalveillance, particulièrement avec les usages de l'intelligence artificielle, qui évolue constamment. Ces sociétés sont les chevilles ouvrières des grandes entreprises et leur fragilité m'interroge.

Enfin, la durée d'un an pour la conservation des données me paraît très courte, sachant que vous disiez qu'il faudrait trois ans pour se mettre en conformité avec la loi. Je rappelle, par exemple, que les relevés de comptes doivent être conservés pendant dix ans. Une durée d'un an est-elle suffisante pour assurer une traçabilité en cas d'enquête ?

M. Vincent Strubel. Les seuils applicables aux entités importantes et essentielles sont prévus par la directive REC. C'est pour cette raison que, dans la version initiale du gouvernement, le projet de loi ne les reprenait pas. Ils ont été ajoutés par le Sénat, dans une logique tout aussi légitime de lisibilité. Je m'en remettrai à votre sagesse sur ce point. D'ailleurs, même s'il était question d'inclure les seuils dans les décrets, seule une paraphrase de la directive serait envisageable, au risque de procéder à une surtransposition qui n'aurait pas lieu d'être.

Cela étant, il faut évidemment se préoccuper des plus petites entités et leur apporter des solutions. L'analyse partagée au niveau européen était que, compte tenu de leur niveau de maturité, il était déraisonnable de leur imposer par la loi des exigences en matière de cybersécurité. Quant aux structures de taille intermédiaire, potentiellement concernées par la directive NIS 2, il convient de les aider à monter en gamme avant d'envisager de les réguler.

Je ne saurais dire s'il faudra un jour réguler les plus petites entités. Le cas échéant, cela demandera une profonde refonte du cadre législatif européen. Appliquer la directive NIS 2 représente déjà une tâche importante. À cet égard, les labellisations qui pourraient être introduites dans ce cadre pourront peut-être être ensuite étendues aux structures plus petites, avec un degré d'exigence similaire ou réduit, en s'appuyant sur le secteur assurantiel ou financier. En effet, un banquier qui prête de l'argent à une très petite entreprise a de plus en plus vocation à se préoccuper du risque cyber. Peut-être fournit-il donc un levier suffisant, sur le

fondement d'un référentiel établi dans ce domaine. Il y a plusieurs pistes de réflexion.

Quant aux règles de conservation des données d'enregistrement des noms de domaine, elles évoluent régulièrement. Ce n'est pas comparable avec les registres de compte et le but n'est pas nécessairement de conduire des enquêtes. Dans la mesure où il s'agit plutôt de répondre aux attaques dans un délai relativement court, il n'y a pas lieu de préconiser une très longue conservation des données, qui sont d'ailleurs assez volumineuses. Il y a un équilibre à trouver et le projet de loi devra certainement faire l'objet d'amendements en ce sens, notamment sur le fondement des retours de l'Afnic.

M. le président Philippe Latombe. Nous vous remercions, monsieur Strubel, de vous être rendu disponible pour cette seconde audition.

II. DISCUSSION GÉNÉRALE

Première réunion du mardi 9 septembre 2025 à 15 heures

La commission spéciale a procédé à la discussion générale sur le 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. Nous nous retrouvons aujourd'hui pour l'examen d'un texte important : le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Ce texte, déposé sur le bureau du Sénat le 15 octobre 2024, a été adopté par la Chambre haute le 12 mars 2025, après engagement de la procédure accélérée par le gouvernement.

Notre commission a consacré un travail long, rigoureux et approfondi à ce projet. Ce travail s'est notamment traduit par un cycle d'auditions dense, organisé entre le 7 mai et le 15 juillet 2025. Quatorze auditions en plénière au total, réunissant près de soixante personnes, nous ont permis de croiser les regards, d'entendre des analyses variées, d'appréhender les enjeux à la fois techniques, juridiques, économiques et stratégiques.

À la demande du rapporteur général, nous avons ouvert et conclu ce cycle d'auditions avec l'Agence nationale de la sécurité des systèmes d'information, l'Anssi, institution incontournable de la politique nationale de cybersécurité. Nous avons également entendu le secrétariat général de la défense et de la sécurité nationale, le SGDSN, dont le rôle de coordination interministérielle est décisif.

Nous avons associé les associations d'élus, qui portent la voix des territoires et qui nous rappellent combien la résilience ne peut être pensée seulement depuis Paris. Nous avons entendu de nombreuses entreprises et associations du secteur numérique et industriel, directement concernées par l'application de ces nouvelles obligations. Nous avons auditionné la Commission nationale de l'informatique et des libertés, la Cnil, garante de nos libertés individuelles dans un contexte où sécurité et protection des données doivent avancer de concert. Nous avons aussi entendu le parquet de Paris, compétent en matière de cybercriminalité, le groupement d'intérêt publique Action contre la cybermalveillance et le Comcyber (commandement de la cyberdéfense) du ministère de l'intérieur. N'oublions pas l'audition consacrée à la régulation financière. Le sujet des télécommunications a été abordé au cours d'auditions dédiées. Enfin, nous avons consacré deux auditions spécifiques à la question du chiffrement, sujet complexe, sensible, mais central pour la confiance numérique et introduit dans le projet de loi par un amendement sénatorial.

Je remercie l'ensemble des personnes auditionnées, ainsi que notre rapporteur général, Éric Bothorel, et nos rapporteurs thématiques pour la qualité et l'intensité du travail accompli.

Notre calendrier politique a été bouleversé par la démission du gouvernement. Mais il importe que notre assemblée puisse poursuivre ses travaux, en particulier sur des textes comme ce projet de loi. En effet, il vise essentiellement à transposer trois directives européennes adoptées en 2022.

D'abord, la directive REC, sur la résilience des entités critiques, acte un changement fondamental : nous passons d'une logique de protection à une véritable approche de résilience face aux risques. Ce sera l'objet du titre Ier du projet de loi, rapporté par Mme Hervieu.

La directive NIS 2 – Network & Information Security – doit élever de manière substantielle le niveau de cybersécurité dans l'ensemble de l'Union européenne en renforçant les obligations des opérateurs et en améliorant la coopération entre États membres. C'est l'objet du titre II, rapporté par Mme Le Hénanff.

Enfin, la directive Dora, le Digital Operational Resilience Act, vise à assurer la résilience opérationnelle numérique du secteur financier, bancaire et assurantiel, dont la sécurité conditionne l'ensemble de l'économie. Ce sera l'objet du titre III, rapporté par M. Bouloux.

Ces transpositions sont urgentes. Les directives REC et NIS 2 auraient dû être transposées avant le 17 octobre 2024. Quant à la directive Dora, elle aurait dû l'être avant le 17 janvier 2025.

Nous sommes donc déjà en retard, et chaque mois qui passe accroît le risque d'infraction de la France par rapport à ses engagements européens. Du reste, la note du secrétariat général du gouvernement sur les contours de la notion d'affaires

courantes de juillet 2024 a rappelé que, si la question de la possibilité juridique d'une activité législative sous l'empire de la Constitution de 1958 était inédite et d'une résolution délicate, l'échéance de transposition d'une directive pourrait justifier une telle activité. Dans ce contexte, notre commission a la responsabilité d'avancer.

La conférence des présidents du 8 juillet dernier avait acté la demande du Gouvernement d'examiner dix-neuf articles selon la procédure de législation en commission. Compte tenu des circonstances, j'ai décidé d'utiliser pour l'ensemble des articles la faculté prévue par le dernier alinéa de l'article 107-1 du règlement de notre assemblée, qui dispose : « À l'issue de l'examen du texte par la commission, […] le président de la commission saisie au fond […] peut obtenir, de droit, le retour à la procédure ordinaire, le cas échéant sur certains articles seulement, au plus tard quarante-huit heures après la mise à disposition du texte adopté par la commission. » La commission pourra ainsi travailler utilement, même en l'absence du gouvernement, tout en garantissant que l'exécutif puisse, le moment venu, amender l'ensemble des articles.

M. Éric Bothorel, rapporteur général. Enfin ! Un an de retard et nous ne sommes pas à l'abri de prendre encore un peu plus de temps que prévu. La transposition de ces directives européennes est un train qui ne cesse de prendre du retard ; ce n'est peut-être pas un train fantôme, mais il est tout de même un peu maudit.

Nous n'avons plus de gouvernement, mais nous n'en examinons pas moins un projet de loi et non une proposition de loi. Précisons d'emblée les choses : nous pouvons étudier ce texte car il s'agit de transposer des directives. Le cadre existe ; nous devons simplement l'adapter aux spécificités françaises.

Dès le début de nos travaux, ma ligne de conduite a été d'éviter la surtransposition comme la sous-transposition des directives NIS 2, Dora et REC. L'absence de gouvernement ne nous autorise pas à nous émanciper du cadre réglementaire européen et de la législation nationale. En ma qualité de rapporteur général, je veillerai à ce que nous restions dans les clous du réel, du possible, voire du constitutionnel.

Le travail avec les rapporteurs thématiques s'est déroulé dans un esprit de collaboration et de confiance. Je reprends à mon compte un grand nombre de leurs amendements et propositions ; je leur laisserai bien évidemment le soin de les défendre. Notre commission est transpartisane, vos rapporteurs sont presque tous bretons et Catherine Hervieu mériterait de l'être.

Je veux d'ores et déjà remercier les administrateurs de l'Assemblée qui ont œuvré dans un calendrier flou, avec un gouvernement – depuis hier – flou et sur une matière parfois floue. En revanche, les menaces, elles, n'ont rien de flou. Si l'on se réfère aux seules actualités du mois dernier, nous mesurons bien l'ampleur de la menace, sous toutes ses formes : le CCAS (centre communal d'action sociale) de la ville de Poitiers ; le logiciel Kairos de France Travail ; le constructeur automobile

Jaguar Land Rover, obligé d'arrêter ses usines ; le Muséum national d'histoire naturelle, contraint d'annuler une exposition ; Naval Group ; les services sociaux du conseil départemental de l'Aude ; Auchan ; Orange et Bouygues Télécom. Grandes et plus petites entreprises, grandes collectivités ou simples CCAS, comme l'a écrit La Fontaine dans « Les Animaux malades de la peste » : « Ils ne mouraient pas tous, mais tous étaient frappés. »

La menace cyber peut nous affecter toutes et tous. Par ce projet de loi, nous devons œuvrer à la résilience de tous les maillons de la chaîne. Ce texte répond à la nécessité de renforcer la résilience de notre économie et de notre société face à une menace qui n'épargne plus personne. Selon Vincent Strubel, cette menace actuellement opportuniste pourrait un jour, dans un contexte géopolitique plus large, s'avérer coordonnée avec des menaces étatiques.

Face à cette situation, l'Europe a collectivement élaboré la directive NIS 2 avec une forte impulsion française. Cette directive complète un paysage normatif européen préexistant, notamment la directive NIS 1, tout en s'inscrivant dans une logique différente. NIS 2 représente un changement d'échelle s'agissant du nombre d'entités régulées. En France, nous passerons de quelques centaines à environ 15 000 entités régulées, avec des ordres de grandeur similaires dans les autres pays européens. NIS 2 n'est pas une évolution de NIS 1 mais un changement d'échelle radical, et nous devons être à la hauteur.

La résilience n'est pas un sujet nouveau ; ces dix dernières années, nous avons œuvré, légiféré. Dès 2015, dans sa stratégie nationale, l'État est parti du constat que s'il était plutôt en mesure de protéger ses propres infrastructures ou les infrastructures vitales du pays, il se devait d'apporter une réponse structurée aux autres composantes de la société, souvent désarmées face à une cybercriminalité en plein essor. C'est de cette volonté qu'est né en mars 2017 le GIP Acyma (groupement d'intérêt public Action contre la cybermalveillance) qui, en octobre 2017, a piloté l'ouverture de la plateforme cybermalveillance.gouv.fr, le dispositif national de sensibilisation, de prévention et d'assistance aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales.

Nous avons renforcé les effectifs de l'Anssi et nous devons poursuivre cet effort au regard des nouvelles compétences que ce projet de loi lui confère. Il existe désormais un parquet spécialisé dans le numérique qui instruit des plaintes contre quelques grands acteurs du numérique. Qui sait ? Demain, le filtre antiarnaque que le président de la République a promis aux Français et que les administrations ne cessent de raffiner administrativement, sera peut-être mis en œuvre.

La sécurisation et la régulation de l'espace numérique progressent mais les attaquants avancent toujours plus vite. Les acteurs du numérique attendent ce projet de loi de précision, de cadrage, de normalisation et d'adaptation du droit européen, et ils le veulent clair et précis. Des investissements seront nécessaires ; les grandes entreprises en ont bien conscience, les collectivités sont assez timorées et nos

concitoyens font probablement preuve d'une grande naïveté sur ces sujets. Ce projet de loi doit ainsi être l'occasion de sensibiliser toutes et tous.

Nous aurons quelques désaccords sur des sujets précis mais, pour l'essentiel, ce texte peut être approuvé par le plus grand nombre des parlementaires. À nous d'être pédagogues et efficaces.

Mme Catherine Hervieu, rapporteure pour le titre Ier. Le titre Ier transpose la directive REC, adoptée en 2022 par le Parlement européen. Cette directive, négociée sous présidence française de l'Union européenne, fixe des standards minimums de résilience aux opérateurs européens. Elle permettra de disposer d'un fort niveau d'harmonisation et de partage d'information entre les États membres de l'Union. La crise environnementale et sociale, et le retour de la guerre sur le continent européen témoignent précisément de l'importance de la coopération transfrontalière en matière de résilience.

Cette directive devait être transposée avant le 17 octobre 2024. En avril dernier, j'avais interpellé le gouvernement sur l'urgence d'inscrire ce texte à l'ordre du jour de l'Assemblée. Or il a privilégié l'inscription de la proposition de loi relative à la réforme de l'audiovisuel public et à la souveraineté audiovisuelle qui affaiblit l'accès à l'information à celle de ce texte relatif à la défense nationale. Je remercie chacun d'entre vous d'être présent en vue d'examiner un texte majeur et sensible.

Le titre Ier du projet de loi révise le dispositif national de sécurité des activités d'importance vitale (SAIV) institué en 2006, pour y intégrer les obligations prévues par la directive et étendre son champ d'application. Il s'applique aux opérateurs d'importance vitale (OIV), publics et privés, qui exploitent les établissements et ouvrages dont l'indisponibilité menacerait la continuité de la vie de la nation ou qui pourraient constituer un danger grave pour la population. Le dispositif concerne environ 300 OIV, dont environ 40 appartenant au secteur de la défense, et 1 500 PIV (points d'importance vitale). Le dispositif repose sur des plans établis par les opérateurs et validés par l'autorité administrative, pour sécuriser les points d'importance vitale. Il est coordonné par le SGDSN et animé par chaque ministre coordonnateur pour leurs secteurs respectifs et décliné à l'échelle territoriale par le préfet de zone de défense et de sécurité.

Afin de préparer l'examen de ce texte, j'ai auditionné une trentaine d'interlocuteurs : les fédérations professionnelles de l'eau, de l'hydrogène et de l'environnement ; une entreprise de réseau ; un préfet ; la DGA (direction générale de l'armement) ; le SGDSN ; la direction de la protection des installations, moyens et activités de la défense (DPID), ainsi que les hauts fonctionnaires de défense et de sécurité du ministère de l'économie, du ministère des armées et du ministère de la transition écologique.

Les interlocuteurs auditionnés ont souligné l'efficacité et la robustesse du dispositif, qui a fait ses preuves face à la menace terroriste ou à l'occasion des Jeux

olympiques et paralympiques. Celui-ci a permis de créer une culture de la sécurité au sein des entreprises et des établissements publics, avec une collaboration efficace entre les services de l'État et les opérateurs.

Le projet de loi renforce le dispositif SAIV, prévoit une analyse des risques par les opérateurs, fusionne le plan résilience avec le plan de continuité de l'activité, élargit le champ des enquêtes administratives aux accès à distance des sites, oblige les opérateurs à signaler les incidents. Il prévoit d'instaurer une commission des sanctions qui acterait le passage d'une logique de sanctions pénales à une logique de sanctions administratives plus efficaces et graduées. Les opérateurs pourront recourir de manière exceptionnelle à des régimes dérogatoires aux marchés publics pour se protéger du risque d'ingérence. En outre, la transposition de la directive étend le dispositif à trois secteurs : réseaux de chaleur et de froid, hydrogène et assainissement de l'eau. Je salue ces mesures qui permettront de renforcer le dispositif, que les opérateurs ont déjà bien compris, sans en modifier l'équilibre global.

Enfin, j'ai fait le choix de déposer plusieurs amendements que j'estime nécessaires pour améliorer le projet tel qu'il a été déposé. Je propose d'ajouter la préservation de l'environnement à la définition d'activité d'importance vitale. L'absence de cette mention me semble un oubli grave, alors même que la plupart des secteurs auxquels le dispositif s'applique sont directement liés à la préservation de l'environnement. Je propose également de mettre en exergue l'importance de l'accès à l'information pour la société en l'ajoutant aux secteurs d'infrastructures critiques. Il me semble également utile d'étendre l'analyse des dépendances aux sous-traitants, ce qui avait été fait en commission spéciale au Sénat. Nous investissons de plus en plus dans l'intelligence économique ; lors des tentatives d'ingérence, les sous-traitants sont une porte d'entrée. Par ailleurs, afin de renforcer l'indépendance des membres de la commission des sanctions, je propose, comme plusieurs d'entre vous, de prévoir que leur mandat ne sera pas renouvelable. Enfin, je tiens à signaler un point de vigilance crucial quant aux moyens financiers et humains des collectivités territoriales : il est impérieux de les soutenir et de les protéger dans la mise en œuvre de ces nouveaux objectifs.

Pour terminer, je tiens à remercier le président, le rapporteur général, mes corapporteurs thématiques, ainsi que les administrateurs et les collaborateurs, pour la qualité du travail fourni durant ces derniers mois.

Mme Anne Le Hénanff, rapporteure pour le titre II. Le titre II transpose la directive européenne NIS 2. C'est peu dire que ce projet de loi est attendu depuis longtemps. Il l'est d'abord par les acteurs de la filière qui s'y préparent depuis plusieurs mois – pour ne pas dire plusieurs années – afin de se hisser au niveau des exigences de la directive. Ce texte est d'ailleurs l'occasion de parler de la cybersécurité, sujet qui pâtit malheureusement trop souvent de sa technicité alors qu'il est d'abord et avant tout un sujet de gouvernance. À cet égard, si nous sommes réunis pour examiner le projet de loi, nous le sommes aussi pour débattre d'un sujet fondamental pour la résilience de la nation.

Ce texte est également attendu par les entités qui se verront appliquer les dispositions du projet de loi. J'ai eu l'occasion de m'entretenir avec de très nombreuses d'entre elles au cours des auditions que j'ai menées entre mai et juillet derniers. Nos échanges ont été l'occasion de rentrer dans le détail des dispositions du projet de loi, de recueillir leurs observations, leurs suggestions et parfois leurs craintes. Et pour cause, le passage de NIS 1 à NIS 2 est un véritable bond en avant. Avec la directive NIS 2, ce seront 15 000 entités qui seront assujetties aux dispositions exigeantes du projet de loi. Une telle évolution ne peut se concevoir sans une préparation adéquate, une association de l'ensemble des acteurs de la filière et des parties prenantes et une sensibilisation accrue. Le projet de loi répond clairement à ces impératifs.

Je ne doute pas que nos débats seront à la hauteur des enjeux. S'il est bien un sujet qui doit toutes et tous nous rassembler, c'est bien la cyber-résilience de la nation, objet même du projet de loi. À la lecture des amendements déposés, je sais que c'est ce qui vous anime.

Je résumerai la philosophie qui a guidé mes prises de position en deux points : d'une part, éviter la surtransposition ; de l'autre, parvenir à une rédaction équilibrée. Tout d'abord, j'ai eu à cœur d'éviter toute surtransposition de la directive dans le projet de loi, ce qui se justifie sur le plan juridique, politique, mais également au regard de l'objectif poursuivi. Il n'est dans l'intérêt de personne de surtransposer. Or plusieurs amendements versent dans cette tendance.

Le second principe est le souci de parvenir à une rédaction équilibrée du texte. De ce point de vue, je salue le travail de nos collègues sénateurs qui ont enrichi le texte à l'occasion de son examen. Nous faisons la loi, ce qui implique de faire du droit, mais nous ne sommes pas des juristes. Nous sommes des élus, donc des politiques, mais le devoir de responsabilité doit nous guider avec, chevillé au corps, l'intérêt général des Françaises et des Français. J'aurai l'occasion d'illustrer mon propos de manière plus concrète lors de l'examen des amendements relatifs notamment aux collectivités territoriales.

Par ailleurs, le titre II du projet de loi ne se contente pas de transposer les dispositions de la directive NIS 2. C'est le cas de certains articles qui ont été inscrits dans la version initiale du projet de loi, mais c'est également le cas d'articles introduits par le Sénat. Je pense notamment à l'article 16 bis sur la proscription de l'affaiblissement du chiffrement dont chacune et chacun connaît l'historique.

Pour conclure, sans surprise j'appellerai à l'adoption des dispositions du titre II et, plus généralement, de l'ensemble du projet de loi. C'est un texte utile, nécessaire et attendu. Il nous revient à toutes et à tous d'être à la hauteur du rendez-vous pour renforcer la cyber-résilience de la nation qui nous permettra de faire face aux défis de demain.

M. Mickaël Bouloux, rapporteur pour le titre III. Le titre III a pour objet la transposition de la directive du 14 décembre 2022 sur la résilience opérationnelle

numérique du secteur financier, dite Dora. Elle-même a pour but de mettre en conformité avec le règlement Dora adopté le même jour plusieurs directives et réglementations sectorielles déjà transposées dans notre droit interne. Il s'agit notamment de la directive DSP 2 concernant les services de paiement dans le marché intérieur ; de la directive Mifid II concernant les marchés d'instruments financiers ; de la directive CRD concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement ; du paquet législatif IFR/IFD sur la surveillance prudentielle ; de la directive OPCVM sur les organismes de placement collectif en valeurs mobilières ; de la directive BRRD établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement ; de la directive « solvabilité II » sur l'accès aux activités de l'assurance et de la réassurance.

En conséquence, le titre III modifie un certain nombre de dispositions du code monétaire et financier principalement, mais aussi du code des assurances, du code de la mutualité et du code de la sécurité sociale en raison de la mise en conformité de la directive « solvabilité II » avec le règlement Dora. Celui-ci renforce les obligations opérationnelles imposées aux entités financières, qu'il s'agisse des différents acteurs du secteur bancaire, des salles de marché ou encore des assurances. Il fixe ainsi un nouveau cadre pour la gestion du risque et des incidents liés aux technologies de l'information et de la communication (TIC) en ce qui concerne les tests de résilience opérationnelle numérique, le partage d'information ou encore l'intervention des autorités compétentes.

Il s'agit donc de dispositions assez techniques qui, parfois, ne font qu'inscrire dans la loi des bonnes pratiques d'ores et déjà mises en œuvre. Il ressort de mes auditions que le secteur financier français n'accuse pas de retard concernant la gestion des risques TIC.

Si l'essentiel des articles du projet de loi initial a été adopté sans modification par le Sénat, quelques sujets, qui font l'objet d'amendements, seront débattus. Je pense notamment à la question de l'autorité destinataire des déclarations des incidents majeurs liés aux TIC et celle des notifications volontaires des cybermenaces importantes émises par les entités financières qui font l'objet, respectivement, des articles 43 A et 45 *bis*. De mes auditions ressort une idée largement partagée : l'Agence nationale de sécurité des systèmes d'information (Anssi) doit être, aux côtés de l'Autorité des marchés financiers (AMF) et de l'Autorité de contrôle prudentiel et de résolution (ACPR), destinataire de ces déclarations, tout en veillant à atteindre l'objectif de simplification des démarches pour les entreprises grâce à un guichet unique ou à un formulaire commun. Il reste donc à trouver la bonne rédaction.

Plus largement, il existe un débat sur l'articulation entre la directive Dora et la directive NIS 2 qui fait l'objet du titre II. Dans un nouvel article 62 A, les sénateurs ont tenu à prémunir les entités financières de tout risque de double assujettissement, malgré la reconnaissance du principe *lex specialis* selon lequel

l'acte sectoriel, en l'occurrence le règlement Dora, l'emporte sur la directive – NIS 2 – lorsque ses exigences ont un effet équivalent à celles prévues par la directive. Ce principe n'est pas forcément simple à appliquer.

Par ailleurs, l'article 58 *bis* vise à inverser la charge de la preuve s'agissant de l'indemnisation par les assurances des dommages causés par les cyberattaques dont peuvent être victimes les entités financières. Le problème est que la rédaction adoptée au Sénat en séance ne semble pas vraiment correspondre à l'intention des sénateurs et des sénatrices, voire d'avoir l'effet inverse à celui qui était recherché. Lors d'une audition, la direction générale du Trésor, l'Anssi et la fédération France Assureurs sont parvenues à s'entendre sur une proposition de rédaction que je défendrai.

Enfin, notre dernier débat portera sur la date d'entrée en vigueur du titre III pour les sociétés de financement, c'est-à-dire, pour résumer, les entreprises qui effectuent des opérations de crédit sans être des banques à proprement parler. Le Sénat a décidé que les exigences prudentielles n'entreront en vigueur qu'à compter du 1er janvier 2030 pour toutes les sociétés de financement, sans distinction de taille, tandis que le projet de loi initial prévoyait un délai d'un an pour les sociétés les plus petites. Nous devons trouver un juste milieu.

M. le président Philippe Latombe. Nous passons aux orateurs des groupes.

M. Aurélien Lopez-Liguori (RN). « La question n'est pas de savoir si vous serez attaqué mais quand » : cette vérité, que tous les experts cyber répètent, s'impose désormais aux institutions, aux entreprises, aux communes. Les cyberattaques ne sont plus l'exception, elles sont devenues la règle. Les hôpitaux paralysés, les administrations bloquées, les mairies prises en otage : voilà la réalité quotidienne. Qu'elles viennent d'États étrangers ou de mafias numériques, ces attaques frappent au cœur de la vie des Français. La menace s'accroît sans cesse puisque, en 2024, l'Anssi a traité près de 4 400 incidents, soit une augmentation de 15 % en un an.

Voilà pourquoi ce projet de loi suscite beaucoup d'espoir. Il représente une véritable opportunité pour notre pays. Il transpose plusieurs textes européens : les directives REC et Dora relatives au secteur financier, et surtout la directive NIS 2, qui aura l'impact le plus important puisqu'elle s'appliquera à 15 000 entités. L'effort immense qui sera demandé à ces entités doit être accompagné avec souplesse, car toutes ne disposent pas des mêmes moyens, mais aussi avec fermeté, en particulier pour celles qui gèrent les données les plus sensibles.

Dans ce contexte, un principe, qui a guidé les amendements que le groupe Rassemblement national a déposés, doit nous servir de boussole : la cybersécurité et la souveraineté sont indissociables. Sans souveraineté, la cybersécurité n'est qu'une illusion. Dépendre de prestataires soumis à des puissances étrangères, c'est s'exposer à leur ingérence. Sans cybersécurité, la souveraineté n'est qu'une façade.

Comment parler d'indépendance nationale si nos infrastructures vitales peuvent être arrêtées par un simple rançongiciel ? Or les gouvernements successifs ne l'ont pas compris ou ont refusé de le comprendre. Nous aurions d'ailleurs aimé débattre de cette question avec Mme Chappaz.

Comment justifier que le conseil et la formation en cybersécurité des ministères aient été attribués à une entreprise canadienne, pour une facture de plusieurs centaines de millions d'euros ? Comment justifier que des entreprises cyber françaises – Sqreen, Sentryo, Alsid – aient été rachetées par des Américains sans aucune réaction de l'État ? Et comment justifier que l'éducation nationale et de nombreux ministères aient recours à des entreprises qui sont soumises à des règles d'extraterritorialité ?

Les gouvernements successifs ont fait mille annonces relatives à notre souveraineté numérique. Malheureusement, très peu d'actes ont suivi. Au Rassemblement national, nous avons une volonté politique, celle de protéger notre souveraineté, notre pays et notre écosystème numérique.

À travers les amendements que nous avons déposés, nous proposons, dans le cadre de la commande publique, de privilégier les entreprises françaises ou européennes s'agissant du traitement des données sensibles. Nous souhaitons ajouter le principe de souveraineté dans la stratégie nationale, ce mot ayant d'ailleurs été inséré par le Sénat. Nous avions également proposé d'instaurer un crédit d'impôt cyber pour accompagner les entreprises dans leur sécurisation ; notre amendement a malheureusement été déclaré irrecevable Enfin, nous proposons de responsabiliser l'administration s'agissant des fuites de données. En effet, il est inadmissible que les données des Français soient compromises sans qu'aucun responsable ait eu à rendre des comptes – je pense par exemple à Pôle emploi, devenu France Travail. Pour que ce texte soit utile, ces mesures doivent être adoptées.

Nous le répéterons lors de nos interventions : sans souveraineté, pas de cybersécurité et, sans cybersécurité, pas de souveraineté. L'absence du gouvernement peut nous offrir davantage de liberté, à nous, législateurs, pour trouver des solutions pour la France, son avenir et nos enfants.

M. Denis Masséglia (EPR). En matière de cybersécurité, nous faisons face à une réalité qui est implacable : les attaques se multiplient, elles frappent partout et personne n'est épargné. Entre 2022 et 2023, les attaques par rançongiciel ont augmenté de 30 %, elles ont touché 34 % des TPE (très petites entreprises) et PME (petites et moyennes entreprises), 24 % des collectivités mais aussi des hôpitaux, des universités et des entreprises stratégiques – soit le cœur de la vie économique, sociale et démocratique.

Face à ce défi, l'Union européenne a pris ses responsabilités en adoptant, en 2022, trois directives majeures – REC, NIS 2 et Dora – que ce projet de loi transpose dans notre droit. C'est un texte attendu, ambitieux et surtout nécessaire.

La directive REC modernise et étend le dispositif de sécurité des activités d'importantes vitales jusqu'ici limité à quelques secteurs – l'énergie, le transport. Il s'appliquera désormais à onze secteurs parmi lesquels l'hydrogène, les réseaux de chaleur ou encore l'assainissement. C'est une avancée majeure pour notre résilience collective.

Avec NIS 2, c'est un véritable changement de paradigme. Nous ne parlons plus de la sécurité de quelques centaines d'infrastructures critiques ; désormais, près de 15 000 entités essentielles ou importantes, publiques comme privées, seront concernées, tout comme les collectivités territoriales.

En 2024, l'Anssi a traité 218 incidents ayant affecté les collectivités, dont 44 au niveau départemental et 39 au niveau régional. Ces chiffres suffisent à rappeler que la cybersécurité n'est pas un sujet théorique ; c'est une menace du quotidien. Le seuil retenu de 30 000 habitants devra faire l'objet d'un débat pour garantir un équilibre entre protection et proportionnalité.

Enfin, le règlement Dora garantira que les banques et les assurances disposent des moyens de résilience indispensables dans un monde où les flux numériques conditionnent la stabilité de nos économies.

Au-delà des transpositions, ce texte soulève trois grands enjeux. Tout d'abord, trouver l'équilibre entre souveraineté numérique et libre concurrence. Certains aimeraient d'ailleurs imposer le recours exclusif à des prestataires français ou européens. Bien entendu, nous partageons l'objectif de souveraineté, mais l'ériger en dogme absolu au détriment de l'efficacité pourrait, ici ou là, fragiliser nos entreprises. Ensuite, il est de notre rôle de garantir que les nouvelles compétences en matière de contrôle confiées à l'Anssi, pilier de notre cybersécurité, s'exerceront avec transparence, dialogue et, surtout, pédagogie. Enfin, s'agissant de la protection des collectivités, celles-ci doivent être mieux armées, mais nous devons éviter de prévoir des obligations qui seraient irréalistes pour les plus petites d'entre elles. Notre travail doit donc être guidé par un principe : protéger sans asphyxier.

Par ailleurs, l'article 16 *bis* interdit par principe toute *backdoor* (porte dérobée) dans les messageries chiffrées. Certes, le chiffrement est essentiel pour protéger la vie privée de nos concitoyens, mais refuser par principe toute coopération avec les services de renseignement pose question. Il faudra, là encore, chercher un chemin d'équilibre.

La cybersécurité n'est pas une option technique, c'est une condition de notre souveraineté, de notre sécurité et de la confiance de nos concitoyens. Le groupe Ensemble pour la République soutiendra ce projet de loi avec la volonté d'améliorer encore son équilibre et son efficacité.

M. Arnaud Saint-Martin (LFI-NFP). Permettez-moi tout d'abord de souligner l'absurdité – le scandale même – qu'une commission spéciale puisse tenir ses travaux au lendemain de la révocation du premier ministre et de son

gouvernement. L'Assemblée nationale ayant décidé que le gouvernement n'était définitivement plus légitime, seules les affaires courantes peuvent encore être traitées par les ministres démissionnaires. Bien que ce projet de loi transpose des directives européennes – REC, NIS 2 et Dora –, il ne relève en rien de l'intendance des affaires courantes, de la formalité administrative. En effet, il touche à des sujets sensibles pour notre pays. Il comporte un ensemble d'articles très politiques qui engagent notre souveraineté pour longtemps. Nous examinons un projet de loi en l'absence de ministre pour répondre : c'est une rupture dans les formes instituées, un accroc légal considérable, un précédent inquiétant. Quand bien même ce texte est important – nous en convenons toutes et tous –, il n'y avait pas d'autres options que d'en reporter l'examen. Or cette option de sagesse n'a pas été retenue. C'est grave, mais soit : examinons donc ce texte dans un contexte dégradé, la veille d'un blocage du pays.

Autant le dire d'emblée, ce projet de loi est nécessaire mais largement incomplet. En particulier, il n'alloue pas les moyens humains, financiers et matériels suffisants à l'Anssi pour accomplir ses nouvelles missions. Ce problème central a été largement souligné.

Ici comme ailleurs, la dilution de l'action publique dans les chaînes d'interdépendance et de sous-traitance qui font la part belle à l'initiative privée fragilise notre souveraineté, surtout lorsque ces acteurs ne sont pas à 100 % français.

Néanmoins, notons certaines avancées, comme l'article 16 bis qui interdit les portes dérobées sur les messageries cryptées, alors que le ministre de l'intérieur démissionnaire avait pourtant tenté de les réintroduire au Sénat, sous prétexte de lutter contre le narcotrafic. Les amendements de suppression de cet article sont inadmissibles : interdire tout mécanisme qui craque le chiffrement des messageries protégées est une exigence fonctionnelle voire démocratique qu'il convient de sanctuariser.

Je le dis en guise d'alerte, ces dispositions, pour utiles qu'elles soient, seront forcément en retard sur les évolutions des menaces cyber d'attaquants qui auront toujours un temps d'avance. La puissance publique n'a pas pris la mesure de ce qui se passe alors que nous vivons dans une société toujours plus en réseau, que nous sommes en interconnexion permanente les uns avec les autres, que les liens sociaux se tissent autour du tout numérique en marche forcée, poussé par les marchands de connectivité, et que l'intelligence artificielle vient de plus en plus se mêler à tout ça. Depuis des années, nous interpellons sur les conséquences de la guerre hybride, des déstabilisations étrangères et des dangers pour la cybersécurité ; sur le fait de pouvoir disposer de cloud souverain sous juridiction française et non soumis aux règles néocoloniales nord-américaines. De même, nous interpellons sur la nécessité absolue de protéger nos câbles sous-marins et nos satellites. Or les gouvernements macronistes prennent du retard ou détraquent les mécanismes de défense.

Alors qu'elle aurait dû lever le pied, la start-up nation a accéléré sa cyber-sujétion : on verse dans le technosolutionnisme en appliquant des correctifs et des

pansements, quand il faudrait donner des moyens, changer de braquet et repenser l'encastrement social, économique et politique des systèmes concernés.

De la fintech à l'edtech, en passant par les services publics en ligne – pas si accessibles –, c'est une fuite en avant. Bien que largement encouragé, ce mouvement nuit à notre souveraineté et, de surcroît, coûte cher aux administrations, aux entreprises de toutes tailles et de tous secteurs et aux particuliers ciblés par les rançongiciels : des dizaines de milliards d'euros sont perdus chaque année à la suite d'attaques.

Son dernier avatar est un mégacampus ultrapolluant de l'IA qu'un fonds émirien finance au nord de ma circonscription. Le champ du petit village seine-et-marnais de Fouju en sera dévasté. J'ai interrogé le gouvernement Bayrou sur les problèmes de souveraineté numérique liés à ce mégacentre de données et pseudo-campus à 50 milliards d'euros, qu'il faudra sécuriser, ainsi que sur son impact environnemental. Malheureusement, les gouvernements actuels sont illégitimes et obsolescents : on pourra attendre encore longtemps la réponse.

Nous avons examiné le texte et déposé des amendements, mais on ne peut pas travailler sur des sujets aussi critiques avec un gouvernement démissionnaire.

Mme Marie Récalde (SOC). Le groupe Socialistes et apparentés prend acte de la décision d'examiner ce texte, certes utile et nécessaire, malgré le contexte incertain et le fait qu'il s'agisse d'un projet de loi et non d'une proposition de loi.

Nous partageons le constat de la hausse et de l'évolution des menaces. Sources d'inquiétude légitime pour nos concitoyens, celles-ci rendent nécessaire la transposition des trois directives européennes relatives au renforcement de la résilience de la nation. Nous devons d'abord chercher à améliorer notre cybersécurité, notamment en élevant la maturité des acteurs, grâce à une nouvelle dynamique vertueuse.

La quatrième orientation de la nouvelle revue nationale stratégique, publiée cette année, prévoit déjà de maintenir une cyber-résilience de premier rang. L'enjeu est grave et les dangers réels, pour les acteurs économiques et pour tous nos concitoyens.

Si nous partageons pleinement l'objectif visé, nous mettons en garde : plusieurs difficultés majeures persistent.

Comment croire à la volonté d'obtenir des résultats quand la loi de finances pour 2025 a diminué les budgets de l'Anssi, de Viginum – service de vigilance et de protection contre les ingérences numériques étrangères – et de la Cnil ? Nous regrettons ces choix budgétaires incompatibles avec l'importance des enjeux. L'Anssi a été particulièrement contrainte cette année : elle avait demandé 35 millions supplémentaires mais le montant de ses crédits a diminué de 3,5 millions. Sa direction estime qu'elle aurait besoin de 50 à 60 équivalents temps

plein (ETP) supplémentaires pour assurer les missions de supervision, de contrôle et d'accompagnement qui lui reviendront en application de NIS 2.

Par ailleurs, à l'issue des auditions, certaines questions demeurent. Nous manquons d'informations concernant le coût des nouvelles dispositions pour les entités concernées : l'application doit être possible financièrement et techniquement, et progressive. Nous veillerons à la pérennisation du financement des centres d'alerte et de réaction aux attaques informatiques (Cert). L'accompagnement des acteurs, nécessaire pour la bonne application des directives, reste insuffisant pour permettre une réelle amélioration de leur maturité cyber. Adopter de nouvelles réglementations sans associer pleinement les acteurs, c'est prendre le risque de l'inefficacité.

L'un des principaux défis à relever pour appliquer NIS 2 consistera à trouver les compétences nécessaires. Le marché de la cybersécurité est déjà sous tension : si la difficulté à trouver des personnes formées persiste, toute ambition sera vaine. Pour résoudre ce problème, nous devrons rendre le parcours plus attrayant pour les jeunes et améliorer les rémunérations, afin d'affronter la concurrence avec le secteur privé. Il faudra veiller en particulier aux territoires ultramarins : confrontés à des difficultés de recrutement prégnantes dans ce domaine, ils sont sous-dotés en ressources humaines. Nous ne pouvons nous satisfaire que la collectivité de Martinique ait besoin d'un an et demi pour recruter un responsable de la sécurité des systèmes d'information.

Dans le domaine de la cybersécurité, on observe un fort déséquilibre entre les industries européenne et extra-européenne. Ce texte doit offrir à l'industrie française l'occasion de reprendre une place centrale. Nous devons nous assurer que les entités privées et publiques qui seront soumises aux nouvelles obligations feront appel à des solutions européennes, sous peine de renforcer la dépendance aux acteurs extra-européens.

Les membres du groupe Socialistes et apparentés soutiendront le texte. Ils défendront toutefois des amendements, visant notamment à insérer la notion d'approche tous risques, à mieux définir le périmètre des entités importantes et à préciser quelles entités pourront délivrer le label de confiance créé lors de l'examen du texte au Sénat.

Mme Virginie Duby-Muller (DR). Depuis 2022, la France a subi de nombreuses cyberattaques, qui ont révélé la vulnérabilité de ses infrastructures critiques, de ses services publics et de ses entreprises. Menées principalement avec des rançongiciels ou des techniques d'hameçonnage de plus en plus sophistiquées, *a fortiori* depuis l'émergence de l'IA générative, ces attaques ont perturbé des services essentiels, abouti à des vols massifs de données personnelles et provoqué des préjudices financiers considérables. La santé, les grands organismes de service et les collectivités territoriales ont été particulièrement touchés.

Les établissements hospitaliers sont devenus des cibles récurrentes. En 2022, le Centre hospitalier sud francilien de Corbeil-Essonnes puis l'hôpital André-Mignot de Versailles ont ainsi été paralysés. En 2023, les attaques contre Viamedis et Almerys, opérateurs de tiers payant, ont compromis les données de plus de 33 millions de personnes. Celle menée contre France Travail en mars 2024 a exposé les informations de 43 millions de demandeurs d'emploi, actuels et passés. En Haute-Savoie, Arthaz-Pont-Notre-Dame et Annecy ont été touchées ; les municipalités comme Sallanches subissent une pression constante, avec une moyenne de 250 000 cyberattaques quotidiennes et des pics allant jusqu'à 800 000. Ces exemples illustrent l'ampleur du risque.

Dues au crime organisé ou à des entités étatiques hostiles, les attaques frappent aussi des secteurs essentiels tels que l'énergie, l'industrie, le système financier et les services de santé. Elles révèlent les failles des systèmes d'information dont dépendent désormais l'économie, les institutions et, *in fine*, notre souveraineté.

Le présent projet de loi est donc nécessaire et urgent. Il transpose enfin – avec près d'un an de retard – les directives européennes REC, NIS 2 et Dora. Il s'agit pour l'essentiel d'un texte d'habilitation confiant des pouvoirs étendus au premier ministre ; heureusement, le Sénat a précisé les contours de la future stratégie nationale de cybersécurité.

Toutefois, je défendrai des amendements concernant trois éléments.

Les plans de résilience des opérateurs d'importance vitale doivent comporter des mesures et des équipements. Cependant, l'article 1332-3 du code de la défense emploie le terme « dispositions », qui renvoie plutôt à des précautions générales. Pour éviter toute ambiguïté et de futurs contentieux, je proposerai d'insérer le mot « dispositifs » afin de préciser clairement qu'il peut s'agir de matériels.

Suivant la recommandation du Conseil d'État, le Sénat a introduit dans le code de la défense une définition de la résilience. Toutefois, celle-ci ne vaut qu'en application dudit code. De plus, NIS 2 prévoit une obligation de cyber-résilience, sans définir ce terme. Il faut combler cette lacune.

Le Sénat a souhaité renforcer la formation des personnels au risque cyber. L'intention est bonne mais la rédaction adoptée pourrait entraîner une surtransposition ainsi que des charges disproportionnées pour les entreprises et les collectivités. L'exigence de sécurité ne doit pas imposer des contraintes irréalistes : nous devons trouver un équilibre.

Hormis ces éléments, les membres du groupe Droite républicaine considèrent que ce texte constitue une transposition efficace, à même de mieux protéger les infrastructures et les citoyens. Nous devrons veiller à ce que les textes d'application paraissent sans délai, malgré le contexte politique, et à mieux acculturer la population à ce domaine.

Mme Sabrina Sebaihi (EcoS). Il est plus que temps de parler de cybersécurité, même si, à mon tour, je regrette d'examiner un texte si important avec un gouvernement démissionnaire.

Pendant que nous débattons, en effet, les cybercriminels n'attendent pas : ils frappent partout, tout le temps, sans relâche. En 2024, deux entreprises françaises sur trois ont subi une cyberattaque ; des hôpitaux ont été paralysés pendant des mois et des millions de données de santé ont été mises en vente sur le *dark web*. Quand un hôpital fonctionne en mode dégradé pendant dix-huit mois, il s'agit non d'une simple défaillance technique mais d'une défaillance de l'État.

Face à l'urgence, que fait ce gouvernement ? Il communique, il promet, et il coupe les crédits. L'Anssi, notre bouclier national, demandait 60 postes supplémentaires, elle en a obtenu zéro ; elle réclamait 35 millions pour sécuriser nos infrastructures, elle n'en a reçu que 27. Dans le même temps, on lui demande de passer de 500 entités supervisées à 15 000. Telle est la gestion macroniste : des injonctions toujours plus lourdes sans jamais 1 euro de plus pour les assumer – le fameux « en même temps ».

Résultat, nous transposons, avec des mois de retard, une directive européenne qui aurait dû l'être en 2024 – que de temps perdu, d'attaques qui auraient pu être évitées, de collectivités et d'hôpitaux laissés seuls face au danger ! Le président de la République explique qu'il veut protéger la France des ingérences étrangères mais aucun moyen n'est donné à ceux qui devraient la défendre.

Les cybercriminels se professionnalisent, opérant comme de véritables multinationales : rançongiciels sur abonnement, attaques en kit, données revendues en quelques heures. Face à cela, nos hôpitaux consacrent moins de 2 % de leur budget au numérique, contre 9 % pour le secteur bancaire. Résultat, 20 % de leur parc informatique est obsolète, seuls 7 % des établissements ont un responsable de la cybersécurité et 4 000 postes restent vacants dans ce secteur. Voilà comment l'État fabrique ses propres vulnérabilités, sur le lit de l'hôpital public déjà agonisant.

Les hôpitaux ne sont pas seuls concernés. Les réseaux d'eau potable et d'électricité, les systèmes de transport, les infrastructures de traitement des déchets sont autant de sites sensibles indispensables à la vie quotidienne et à la sécurité de la population. Une cyberattaque sur une station d'eau, sur une centrale électrique ou sur une usine de retraitement ne ferait pas seulement disparaître des données, elle mettrait des vies en danger. Or ces infrastructures vitales sont elles aussi sous-financées et trop souvent livrées à elles-mêmes.

Les collectivités locales, quant à elles, sont en première ligne mais souvent dépourvues d'équipes, d'expertises et de moyens. Les centres régionaux d'assistance financés par France Relance risquent de fermer faute de crédits. Demain, des régions entières seront des déserts cyber. On impose des normes mais on coupe l'assistance : voilà la fameuse résilience vantée par le gouvernement maintenant démissionnaire.

Sans un plan d'investissement massif, ce texte n'est qu'une coquille vide. Le choix politique du gouvernement est limpide : on trouve des milliards pour les

grandes entreprises mais on laisse les collectivités, les hôpitaux et les PME sans défense. On subventionne les dividendes mais on abandonne nos infrastructures vitales ; on protège les bilans des grands groupes, non les vies des citoyens.

La cybersécurité n'est pas un gadget technique ; c'est une condition de souveraineté, de démocratie et de survie. Elle est nécessaire à la continuité des services publics, à la sécurité des données et à la confiance dans les institutions. Elle mérite qu'on déploie une vraie stratégie nationale, financée et ambitieuse, à même de protéger les hôpitaux, les communes et les entreprises. Nous demandons non une France des slogans mais une France qui protège réellement, qui place la cybersécurité au cœur de sa souveraineté, en y consacrant des moyens financiers et humains.

Mme Sabine Thillaye (Dem). Tous les ans, l'Anssi publie un panorama de la cybermenace ; chaque fois le constat est le même, celle-ci se renforce et se diversifie. Elle n'épargne plus aucun secteur de la vie économique et sociale. En 2024, 34 % des cyberattaques ont visé des TPE et des PME ; 24 % des collectivités territoriales ; 10 % des entreprises stratégiques ; 10 % des établissements de santé. Ces chiffres parlent d'eux-mêmes : le risque cyber est systémique et touche tous les secteurs de notre société.

Face à ce constat, l'Union européenne a adopté en 2022 les directives NIS 2, REC et Dora. Ensemble, elles instaurent une logique de résilience globale et cohérente, renforçant la souveraineté numérique européenne. Certains de nos voisins, comme la Belgique et l'Italie, ont déjà transposé NIS 2. En France, les entités concernées n'ont pas attendu pour s'adapter. Toutefois, dans un souci d'harmonisation, de cohérence et de clarté, nous devons mener ce travail législatif à bien le plus rapidement possible.

Nous devons toutefois veiller à éviter toute surtransposition inutile qui entraînerait des surcoûts pour les acteurs concernés, nuirait à la compétitivité de nos entreprises et, finalement, compromettrait l'harmonisation européenne, laquelle doit être notre premier objectif.

Il faudra que les acteurs concernés soient suffisamment accompagnés pour déterminer rapidement s'ils sont assujettis aux obligations prévues dans les directives et pour mettre à niveau leurs systèmes d'information. Il faut garder à l'esprit que le coût, estimé entre 3 et 6 milliards d'euros, est significatif. C'est pourquoi nous devrons débattre du seuil d'assujettissement des collectivités et de l'opportunité de désigner, au sein des communautés de communes, un référent capable d'accompagner ces transformations.

Le Conseil d'État a estimé que le projet de loi était globalement fidèle aux directives, l'exception la plus notable étant l'exemption de sanctions pour les collectivités territoriales et leurs établissements publics, administratifs et groupements qui ne respecteraient pas leurs obligations. Nous devrons débattre des points de divergence sans remettre en cause l'équilibre du texte.

Les membres du groupe Les Démocrates soutient ce projet de loi indispensable pour renforcer la souveraineté numérique européenne. Nos débats sont aussi l'occasion d'appeler l'attention du plus grand nombre sur la nécessité de renforcer la cybersécurité et d'améliorer notre acculturation à ce domaine : chacun d'entre nous a un rôle à jouer pour la défendre.

M. Vincent Thiébaut (HOR). La menace cyber n'est plus une hypothèse lointaine, c'est une réalité quotidienne. Chaque semaine, des attaques ciblées, denses et technologiquement avancées frappent fort les hôpitaux, les collectivités, les opérateurs d'énergie, les entreprises stratégiques et même les administrations.

Le projet de loi vise à apporter à ce problème une réponse claire en transposant trois textes européens majeurs : REC, NIS 2 et Dora. Il s'agit de dessiner une architecture de protection commune. C'est un tournant pour nos services vitaux, nos services financiers, nos infrastructures stratégiques, qui devront adopter les mêmes standards de sécurité et de résilience partout sur le continent.

Le texte tend à protéger les activités indispensables au quotidien des Français, qu'il s'agisse de la santé, de l'énergie, des transports, de l'alimentation ou des communications. Si, à cause d'une attaque, elles devaient s'arrêter, le pays se trouverait en grande difficulté. En renforçant les obligations de prévention, de détention et de réaction, le projet de loi donne aux citoyens de nouvelles garanties.

C'est aussi un projet de loi d'accompagnement, pour les grandes entreprises, souvent déjà bien armées, ainsi que pour les collectivités territoriales, en particulier pour les petites structures qui ont besoin de soutien pour se conformer aux nouvelles obligations. Nous défendrons ainsi des amendements relatifs à l'accompagnement financier, qui peut se révéler essentiel.

Ce texte n'est pas seulement défensif, il est tourné vers l'avenir ; il constitue une occasion formidable de structurer et de renforcer notre filière cyber nationale et européenne. Si nous ne disposons pas encore de tous les acteurs indispensables en Europe, ce texte nous aidera à structurer une filière complète. Les labels de confiance, les partenariats public privé et la mobilisation des expertises locales contribueront à bâtir l'autonomie stratégique dont nous avons cruellement besoin. La cybersécurité n'est pas seulement un coût ; elle est un atout pour la compétitivité de notre économie.

Enfin, c'est important pour nous, ce texte illustre la méthode de la sobriété normative : pas de surtransposition ni de complexité inutile – en tout cas, c'est le cap que nous nous sommes fixé. Il vise à établir une transposition fidèle, proportionnée et pragmatique ; il faut que les obligations imposées aux entités soient adaptées à leur taille et au niveau de risque encouru car c'est la condition d'une application rapide et efficace.

Les membres du groupe Horizons soutiendront ce texte essentiel. Nous attendons les discussions avec impatience, en particulier sur certaines dispositions

introduites par le Sénat, comme celles relatives aux *backdoors* – il est essentiel de pouvoir en débattre paisiblement.

M. Laurent Mazaury (LIOT). Une faille numérique, un mauvais clic, et tout un service peut s'arrêter : c'est la réalité de la cybermenace que ce projet de loi tend à combattre.

En 2024, nos entreprises, nos administrations et nos collectivités ont totalisé 384 000 atteintes numériques, notamment pendant les Jeux olympiques, soit une hausse de 75 % en cinq ans. Le préjudice annuel est estimé à 2 milliards d'euros.

Il est donc plus que temps de transposer les trois directives européennes de 2022 – REC, NIS 2 et Dora. Derrière son aspect technique, ce texte doit marquer une étape décisive du renforcement du bouclier cyber de l'État et des entreprises – de la France.

S'agissant de la résilience des activités d'importance vitale, nous ne partons pas de rien : le dispositif SAIV compte déjà 300 opérateurs. Notre groupe salue son extension à de nouveaux secteurs essentiels, comme l'assainissement et l'hydrogène.

Les opérateurs concernés auront de lourdes obligations, en particulier l'établissement d'un plan de résilience. Même si ces mesures sont indispensables, il faudra leur laisser suffisamment de temps pour les appliquer.

Les sanctions sont utiles mais il faut raison garder. Le texte prévoit des amendes pouvant atteindre 2 % du chiffre d'affaires mondial. Je défendrai un amendement visant à mieux les calibrer et à éviter l'une de ces surtranspositions dont notre pays a le secret. Par ailleurs, l'État devra accompagner les acteurs et agir en partenariat avec les opérateurs stratégiques.

La transposition de NIS 2 fait passer le nombre des entités dites essentielles ou importantes, donc régulées, de 500 à près de 15 000 ; 1 300 collectivités, dont 300 communes, seront désormais concernées. Un tel changement constitue un défi.

Nos services de proximité sont vulnérables ; les mairies, les services départementaux d'incendie et de secours (Sdis), les hôpitaux sont de plus en plus visés. Une cyberattaque qui bloque un service d'urgence n'est pas un simple bug : c'est une menace directe pour la population. Il ne s'agit pas de fiction : l'hôpital André-Mignot, dans les Yvelines, s'est trouvé bloqué du jour au lendemain ; trois ans après, son fonctionnement quotidien s'en ressent encore.

Transposer des directives n'est pas tout : il faudra aussi territorialiser la nouvelle stratégie nationale pour la cybersécurité, en la dotant d'un échéancier et, surtout, de financements, car les acteurs locaux ont besoin de visibilité. Nous appelons à offrir un accompagnement spécifique aux élus locaux. La prise de conscience a eu lieu mais, la Cour des comptes le souligne dans son rapport consacré à la réponse de l'État aux cybermenaces sur les systèmes d'information civils paru

en 2025, il reste trop difficile de se retrouver dans la foison de dispositifs. L'Anssi, dont le texte confirme le rôle de chef de file, doit assurer un accompagnement unifié et clair.

Il faut être lucide quant aux menaces extérieures et intérieures, et ne rien nous interdire pour sauvegarder la sécurité de la France. Pour cette raison, je défendrai la suppression de l'article 16 *bis*. Il faut non céder à la peur mais affronter la cybermenace. Parce que ce projet de loi est attendu, nécessaire et responsable, notre groupe le soutiendra.

M. Édouard Bénard (GDR). Examiner ce texte, dans les conditions dégradées que nous connaissons, sans ministre, est aberrant. Un projet de loi de cette ampleur, relatif à la cybersécurité, ne relève pas de la gestion des affaires courantes.

Depuis la fin du XX^{e} siècle, la numérisation accélérée et la dépendance croissante aux technologies de l'information et de la communication ont profondément transformé les infrastructures économiques et financières. Cette évolution s'est accompagnée d'une concentration inédite des ressources et des services stratégiques entre les mains d'un oligopole de grandes entreprises, extra-européennes pour la plupart. Un tel déséquilibre limite directement la capacité de nos États à intervenir et à définir leur modèle de production et d'innovation industrielle.

Parallèlement, l'économie des données est devenue le socle de nouveaux marchés. Les données produites par les usagers, collectées, transformées, exploitées puis commercialisées, sont désormais une matière première du capitalisme contemporain.

Le numérique occupe donc une place centrale, avec pour conséquence redoutable l'essor massif de la cybercriminalité. La guerre économique se déroule désormais dans le cyberespace, et les attaques sont multiformes : intrusions orchestrées par des puissances étatiques, rançongiciels déployés par des groupes criminels, campagnes de manipulation informationnelle, espionnage industriel. Selon le gouvernement, le coût moyen d'une cyberattaque s'élève à 14 000 euros par entreprise.

En 2022, 385 000 attaques ont réussi, provoquant une perte globale de 2 milliards d'euros. Un dixième concernait des organismes publics. À peine 0,2 % a été déclaré à l'Anssi. Face à cette menace, le présent projet de loi transpose trois directives européennes – REC, NIS 2 et Dora – pour renforcer la sécurité des systèmes d'information. Il prévoit de nouvelles obligations de déclaration et tend à garantir une meilleure surveillance des prestataires critiques. Il monte à 14 500 le nombre des entités que l'Anssi sera chargé de suivre et de contrôler.

Ces avancées, réelles et nécessaires, ne suffisent pas. Le texte ne concerne que l'aval de la chaîne : les logiciels, les réseaux, les obligations de conformité. L'amont, à savoir la maîtrise des infrastructures matérielles stratégiques

– production de puces, data centers et technologies de calcul quantique notamment – reste ignoré. Les secteurs concernés demeurent sous domination extra-européenne. Trois acteurs américains, Amazon, Microsoft et Google, détiennent 70 % du marché européen du cloud. Cette dépendance constitue un risque majeur pour notre souveraineté numérique.

Les nouvelles obligations pèseront lourdement sur les petites structures, en particulier les TPE et les PME, qui ne disposent ni des moyens humains ni des compétences techniques nécessaires pour les assumer – elles n'ont pas les capacités d'adaptation des grands groupes.

Il est indispensable de bâtir les conditions d'une autonomie numérique européenne. Pour y parvenir, il faut réinternaliser une partie des infrastructures stratégiques, investir dans nos propres data centers et solutions cloud et réduire notre dépendance aux acteurs extra-communautaires. À défaut, notre cybersécurité restera fragile et, face aux grandes puissances technologiques, nos marges de manœuvre limitées.

M. le président Philippe Latombe. Nous en venons à une intervention à titre individuel.

Mme Laetitia Saint-Paul (HOR). Je craignais que ce texte ne soit la première victime collatérale du vote de défiance d'hier. La quantité des attaques, leur qualité, l'effondrement de leur prix et la diversité des modes d'action sont tels que nous n'avons plus une minute à perdre. Je salue donc, monsieur le président, votre décision d'avoir maintenu l'examen du texte.

Par ailleurs, je soutiens la volonté de la rapporteure Anne Le Hénanff de tout faire pour éviter la surtransposition : nous avons besoin d'un texte opérationnel à l'échelle européenne.

III. EXAMEN DES ARTICLES DU PROJET DE LOI

1. Deuxième réunion du mardi 9 septembre 2025 à 16 heures 30

La commission spéciale a procédé à 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. La commission a été saisie de 530 amendements. En application de l'article 45 de la Constitution, j'en ai déclaré irrecevables vingt-sept, qui ne présentaient aucun lien, même indirect, avec les dispositions du projet de loi initial. J'ai notamment estimé que tous les amendements dont le dispositif relevait directement du règlement général sur la protection des données (RGPD) ou de la loi de programmation militaire (LPM)

étaient des cavaliers. En vertu de l'article 40 de la Constitution, le président de la commission des finances, Éric Coquerel, a déclaré irrecevables les amendements tendant à créer une charge pour les finances publiques.

Suivant la pratique de plusieurs commissions permanentes, nous examinerons en fin de discussion les amendements visant à obtenir du gouvernement un rapport, afin de faire preuve de discernement en la matière.

TITRE IER
RÉSILIENCE DES ACTIVITÉS D'IMPORTANCE VITALE

CHAPITRE IER
DISPOSITIONS GÉNÉRALES

Article 1er : (art. L. 1332-1 à 6 et art. L. 1332-7 à 22 [nouveaux] du code de la défense) *Transposition de la directive 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des activités critiques (REC)*

Amendements identiques CS264 de Mme Catherine Hervieu et CS162 de Mme Sabrina Sebaihi

Mme Catherine Hervieu, rapporteure. La préservation de l'environnement est essentielle à la survie de la nation. Pourtant, l'alinéa 7, qui définit les activités d'importance vitale, ne la mentionne pas. Ces amendements tendent à y remédier.

Le point 478 de la revue nationale stratégique indique explicitement qu'il faut donner une plus grande place au risque environnemental dans le dispositif.

Le ministère de la transition écologique, de la biodiversité, de la forêt, de la mer et de la pêche est déjà responsable d'environ 50 % des opérateurs visés. La précision est donc cohérente.

M. Éric Bothorel, rapporteur général. La notion d'environnement n'est pas étrangère aux activités d'intérêt vital, mais la mention de sa préservation n'est pas totalement cohérente avec les objectifs concrets de sécurisation. De plus, elle est déjà présente dans celle d'activité indispensable au fonctionnement de la société.

En créant un inventaire à la Prévert, on prend le risque d'oublier certains éléments, qui ne seront dès lors pas considérés comme indispensables.

Je vous invite donc à retirer ces amendements ; à défaut, j'émettrai un avis défavorable.

Mme Catherine Hervieu, rapporteure. La directive REC dispose qu'est « essentiel » un service crucial pour le maintien de l'environnement. La définition que je propose est donc conforme au droit européen.

M. Éric Bothorel, rapporteur général. Je ne pointe pas un défaut de cohérence mais l'inutilité de la précision. L'environnement est déjà pris en considération. La présence de onze secteurs relevant du ministère de la transition écologique, étroitement liés à cette question, le montre.

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

Amendement CS196 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Les institutions, qui sont la cible privilégiée des ingérences étrangères – cyberattaques contre les mairies, l'Assemblée nationale, France Travail ; tentatives de manipulation électorale, de déstabilisation –, ne figurent pas dans la définition actuelle des infrastructures critiques. Il est proposé de combler ce vide.

M. Éric Bothorel, rapporteur général. L'objectif de préservation du fonctionnement des institutions est pris en compte dans la définition des activités d'importance vitale car toute perturbation heurterait nécessairement le fonctionnement de la société. Votre amendement étant satisfait, j'en demande le retrait ; à défaut, avis défavorable.

Mme Catherine Hervieu, rapporteure. Le fonctionnement des institutions est sous-entendu par la définition d'une infrastructure critique. Avis défavorable.

*L'amendement est **retiré**.*

Amendements identiques CS265 de Mme Catherine Hervieu et CS163 de Mme Sabrina Sebaihi

Mme Catherine Hervieu, rapporteure. Il est proposé d'ajouter à la définition de l'infrastructure critique la notion d'accès à l'information, afin de souligner l'importance vitale pour la société des médias, de l'audiovisuel et de la presse. Les infrastructures nécessaires à la diffusion de l'information aux citoyens doivent être considérées comme critiques pour assurer leur résilience.

Mme Sabrina Sebaihi (EcoS). Les attaques visent non seulement les hôpitaux et les réseaux d'énergie, mais aussi les esprits et notre démocratie, par la désinformation, les *fake news* et les manipulations orchestrées parfois depuis l'étranger. Inscrire l'accès à l'information dans la définition des infrastructures critiques, c'est reconnaître que sans information libre, fiable et protégée, notre société devient vulnérable aux ingérences et aux propagandes. Ce n'est pas un luxe : nous devons bâtir un rempart contre les dérives.

M. Éric Bothorel, rapporteur général. Vous avez raison : c'est loin d'être un luxe. C'est la raison pour laquelle cette disposition figure déjà dans certaines directives nationales de sécurité. Demande de retrait et, à défaut, avis défavorable.

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

Amendements identiques CS465 de M. Éric Bothorel et CS448 de Mme Catherine Hervieu

Mme Catherine Hervieu, rapporteure. Il s'agit de clarifier la notion d'infrastructure critique utilisée en droit européen. La directive REC adopte une définition de la notion d'infrastructure critique plus large que la notion de point d'importance vitale utilisée en droit national et bien appréhendée par les opérateurs. Le projet de loi, par l'emploi de l'adverbe « notamment », a fait le choix de conserver le périmètre actuel des PIV et de concevoir ces derniers comme une catégorie spécifique d'infrastructures critiques au sens de la directive.

Toutefois, la multiplication récente des textes européens faisant référence à la notion d'infrastructure critique rend de moins en moins pertinente la distinction entre, d'une part, les infrastructures qui correspondraient aux PIV et aux SIIV (systèmes d'information d'importance vitale) et, d'autre part, des infrastructures critiques qui en seraient exclues. Pour des raisons de cohérence entre le droit européen et le droit interne, il apparaît souhaitable de lever toute ambiguïté en supprimant l'adverbe « notamment », afin d'assurer une identité entre, d'un côté, les PIV et les SIIV, et, de l'autre, les infrastructures critiques.

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

Amendement CS125 de Mme Catherine Hervieu et sous-amendement CS482 de Mme Virginie Duby-Muller

Mme Catherine Hervieu, rapporteure. Il s'agit de corriger une erreur de syntaxe dans la définition de la résilience. « Prévenir contre tout type d'incident » est une formulation incorrecte. Il est proposé de définir la résilience comme « la capacité d'un opérateur à prévenir tout type d'incident, à s'en protéger et à y résister ».

Mme Virginie Duby-Muller (DR). Le sous-amendement vise à compléter la définition de la résilience en y intégrant explicitement la capacité de se rétablir après un incident, prévue par la directive. Sans cette mention, notre droit national offrira une définition incomplète qui risquerait de ne pas rendre justice à l'esprit du texte européen.

Le rétablissement n'est pas un élément secondaire : il constitue une condition essentielle de la continuité des activités critiques. Les crises cyber, les catastrophes naturelles ou encore les incidents techniques ne peuvent être considérés comme maîtrisés que si l'activité normale peut être restaurée rapidement et efficacement. En ajoutant ces quelques mots, nous apportons une clarification utile qui renforce la cohérence juridique de notre droit avec la directive.

Mme Catherine Hervieu, rapporteure. La notion de « continuité de l'activité », davantage utilisée en droit national et qui a la préférence du SGDSN, figure déjà dans la définition. Avis défavorable.

Le sous-amendement est ***retiré****.*

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

Amendement CS197 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Il n'existe aucune définition légale de la souveraineté numérique. En conséquence, ce concept assez flou demeure difficile à appliquer et à contrôler. L'amendement en propose donc une définition claire : la capacité de l'État à fixer les règles, à assurer son autonomie technologique et à se protéger des ingérences étrangères.

Une définition complète constituerait une boussole juridique stratégique ; elle permettrait de guider nos politiques numériques et de mettre fin aux abandons de souveraineté que nous consentons depuis des années. Aujourd'hui, les grands ministères ont toujours recours à une entreprise canadienne pour assurer la formation en cybersécurité : ce n'est pas normal. En fixant une définition de la souveraineté numérique, nous parviendrons peut-être à nous extirper de cette situation.

Mme Catherine Hervieu, rapporteure. Les définitions présentes dans le projet de loi sont issues de l'article 2 de la directive REC, transposé par l'article 1er. Elles ont pour objet de poser le cadre du dispositif de sécurité des activités d'importance vitale, lequel n'utilise pas la notion de souveraineté numérique. Un tel ajout à l'article 1er du projet de loi constituerait alors une surtransposition, qui pourrait ouvrir la voie à des conséquences néfastes pour le dispositif global. Avis défavorable.

M. Éric Bothorel, rapporteur général. Si personne ici ne s'oppose à l'idée qu'il faut conquérir la souveraineté numérique, inscrire sa définition dans le présent texte constituerait une surtransposition qui créerait de l'insécurité juridique pour les entreprises. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). Nous ne sommes pas le seul groupe à avoir déposé des amendements relatifs à la souveraineté numérique dans ce texte. Il me paraît possible de trouver une majorité pour l'adoption de certains d'entre eux. Inscrire une définition de la souveraineté numérique dès l'article 1er permettrait de clarifier cette notion et de renforcer la directive telle qu'elle sortira de nos travaux.

Mme Catherine Hervieu, rapporteure. La souveraineté numérique n'entre pas dans le dispositif envisagé. Votre amendement irait à l'encontre de l'objet du texte, qui vise seulement à transposer la directive en droit national.

M. Éric Bothorel, rapporteur général. La souveraineté numérique devra probablement être définie un jour. Nous aurons ce débat, notamment avec ceux qui réclament la souveraineté numérique mais ne veulent pas des infrastructures chez eux. Ce sujet est sérieux et mérite mieux qu'une discussion au détour de l'examen d'un texte de transposition.

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

Amendement CS42 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). L'amendement tend à imposer aux opérateurs d'importance vitale et aux entités critiques des dispositifs visant à protéger les personnes travaillant en leur sein. Il s'agit pour les OIV de tenir compte des risques psychosociaux et organisationnels auxquels sont soumis des agents en situation de stress élevé dans les plans de continuité ou de rétablissement d'activité exigés des opérateurs. L'expérience récente a démontré que l'absentéisme, la désorganisation managériale et l'épuisement professionnel pouvaient gravement compromettre la continuité de services pourtant techniquement robustes. Cet amendement s'inscrit dans une logique de résilience globale incluant le facteur humain, en cohérence avec les recommandations émises par plusieurs autorités de régulation et agences nationales de sécurité.

Mme Catherine Hervieu, rapporteure. S'il est indispensable de prévoir des mesures d'accompagnement et de limitation des risques auxquels sont exposés les salariés en cas de crise, le plan de résilience opérateur ne me semble pas être le bon véhicule pour prendre en compte les risques psychosociaux pour deux raisons principales. Tout d'abord, le plan étant classifié, ses éléments ne seront pas accessibles à l'ensemble des salariés et les syndicats auront un droit de regard très limité. La portée des mesures serait ainsi très réduite.

Ensuite, le plan devant être validé par l'autorité administrative, la préfecture devrait approuver ou modifier des mesures d'accompagnement des salariés, ce en quoi elle n'est pas compétente. Il serait donc plus judicieux de traiter ces sujets au sein des instances dédiées au dialogue social de chacune des entreprises concernées. Néanmoins, je partage tout à fait votre point sur l'importance d'inclure les risques pyscho-sociaux. Avis défavorable.

M. Éric Bothorel, rapporteur général. Les mesures proposées sont excessives car l'ensemble des employés d'un OIV serait concerné, alors que la qualification d'OIV peut n'être justifiée que pour une partie de ses activités. Je m'aligne donc sur l'avis de Mme la rapporteure.

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

Amendements CS101 de M. Arnaud Saint-Martin, CS446 de Mme Catherine Hervieu et CS198 de M. Aurélien Lopez-Liguori (discussion commune)

M. Arnaud Saint-Martin (LFI-NFP). L'amendement CS101 vise à renforcer l'analyse des dépendances et des vulnérabilités des opérateurs d'importance vitale et de leurs sous-traitants en intégrant une approche globale de la sécurité, incluant la chaîne d'approvisionnement complète et la circulation des ressources humaines et matérielles.

Cette évaluation doit prendre en considération la dépendance à des prestataires ou fournisseurs stratégiques, y compris pour les services de logistique, de maintenance et de numérique, les conditions d'accès aux infrastructures, aux systèmes d'information et aux données sensibles, en distinguant les accès permanents, temporaires ou à distance, les flux de mobilité du personnel intervenant sur plusieurs sites, ainsi que les risques associés au transport et au stockage hors site d'équipements ou de supports d'information.

Mme Catherine Hervieu, rapporteure. L'amendement CS446 vise à intégrer les vulnérabilités des sous-traitants dans l'analyse des dépendances réalisée par les opérateurs d'importance vitale. L'interdépendance croissante de l'économie nécessite de leur part une analyse détaillée des vulnérabilités de leur chaîne d'approvisionnement. Or celle-ci ne peut être complète sans prendre en compte les sous-traitants, dans une démarche analogue à celle prévue par la directive de 2022 sur le devoir de vigilance des entreprises.

Je propose de réintroduire cette disposition qui avait été ajoutée en commission au Sénat, puis supprimée en séance. Afin d'éviter de surcharger les opérateurs, l'analyse serait réalisée dans un délai plus long que celui prévu par la directive REC ; il serait fixé par voie réglementaire.

M. Aurélien Lopez-Liguori (RN). Le Sénat a commis une erreur stratégique en supprimant l'obligation pour les OIV d'analyser les vulnérabilités de leurs sous-traitants. Les cyberattaques passent de plus en plus par la chaîne de sous-traitance, plus fragile. Il en existe de nombreux exemples : l'attaque de SolarWinds par un logiciel tiers a permis d'infiltrer des milliers d'organisations, dont des agences de l'État américain ; le rançongiciel NotPetya, propagé par une simple mise à jour d'un logiciel de comptabilité, a paralysé des entreprises du monde entier ; en France, plusieurs collectivités locales et établissements de santé ont été victimes d'attaques passées par des prestataires techniques insuffisamment protégés.

Supprimer cette exigence revient à se priver d'un bouclier indispensable et à sacrifier la sécurité à des impératifs pratiques ou économiques de court terme. Notre souveraineté numérique repose autant sur les grands opérateurs que sur la solidité de l'écosystème qui gravite autour. Les attaquants ont compris que la sous-traitance était leur cheval de Troie. Nous voulons donc rétablir le contrôle de la sous-traitance.

Mme Catherine Hervieu, rapporteure. L'amendement CS101 vise à étendre l'analyse des dépendances aux sous-traitants et aux accès physiques et numériques. Je suis favorable à l'intégration des sous-traitants dans l'analyse, sous réserve d'accorder un délai supplémentaire aux opérateurs. En revanche, intégrer les accès physiques et numériques et les équipements dans cette analyse aurait peu de sens dans le dispositif tel qu'il est conçu. Avis défavorable.

Concernant l'amendement CS198, un délai supplémentaire s'impose pour l'analyse des dépendances des sous-traitants. Avis défavorable.

M. Éric Bothorel, rapporteur général. Le dispositif prévu par la directive REC traite de la chaîne d'approvisionnement, qui couvre la question de la sous-traitance. Les trois amendements opèrent donc une surtransposition. Avis défavorable.

Mme Catherine Hervieu, rapporteure. L'argument de la surtransposition sera sans doute le fil rouge de nos débats. La fragilité de la sous-traitance est un point de vigilance et le fait d'accorder un délai pour qu'elle soit alignée correctement sur la chaîne de valeur enverrait le signal qu'elle est bien intégrée dans le dispositif. Cela ne me semble pas constituer une réelle surtransposition.

Successivement, la commission ***rejette*** *l'amendement CS101 et* ***adopte*** *l'amendement CS446.*

En conséquence, l'amendement CS198 ***tombe****.*

Amendement CS450 de M. Philippe Latombe

M. le président Philippe Latombe. Il s'agit d'intégrer, dans le périmètre de l'analyse des risques, les dépendances à l'égard des tiers et les vulnérabilités dans la chaîne d'approvisionnement. Cela vise à clarifier la question de la dépendance technologique vis-à-vis de fournisseurs de solutions logicielles et matérielles propriétaires.

Je réponds par avance à l'argument de la surtransposition en rappelant que, lors de l'adoption de la directive, nous n'avions pas encore connu ce qu'il s'est passé récemment avec les États-Unis : la possibilité pour un gouvernement d'utiliser un *kill switch* pour empêcher le bon fonctionnement d'un système en stoppant les mises à jour. Cela s'est matérialisé très concrètement, il y a quelques jours, par un *executive order* du président Trump à l'encontre de quatre juges de la Cour pénale internationale. Je souhaite donc compléter l'alinéa 32 pour que l'analyse des risques assure une visibilité du risque de *kill switch* pour l'ensemble des infrastructures concernées.

Mme Catherine Hervieu, rapporteure. Il est bénéfique de s'assurer que l'analyse des dépendances prenne en compte la dimension numérique pour garantir la continuité de l'activité des opérateurs. Avis favorable.

M. Éric Bothorel, rapporteur général. Sagesse.

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

Amendement CS126 de Mme Catherine Hervieu

Mme Catherine Hervieu, rapporteure. Rédactionnel. L'amendement reformule la définition du plan particulier de résilience en remplaçant le pluriel par du singulier s'agissant de la mention de l'opérateur d'importance vitale.

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

Amendements identiques CS478 de M. Éric Bothorel, CS9 de Mme Virginie Duby-Muller et CS452 de M. Philippe Latombe

Mme Virginie Duby-Muller (DR). Il s'agit d'intégrer explicitement la mention des dispositifs dans le plan particulier de résilience des opérateurs d'importance vitale. En l'état, le texte ne fait référence qu'aux procédures, sans distinguer clairement ce qui relève des équipements, d'une part, et des dispositifs et des procédures, d'autre part. Or un plan particulier de résilience doit être exhaustif pour être pleinement opérationnel. Il s'agit non seulement de prévoir des protocoles mais aussi d'identifier les moyens matériels et techniques indispensables à leur mise en œuvre.

L'ajout proposé assure la cohérence avec l'esprit de la directive REC, qui insiste sur la nécessité de garantir la continuité effective des services essentiels, et renforce la lisibilité du plan de résilience pour l'autorité administrative chargée de l'approuver. Il s'agit d'un amendement de clarification et de sécurisation juridique et opérationnelle.

Mme Catherine Hervieu, rapporteure. Ces amendements apportent une distinction utile en précisant les mesures qui relèvent d'équipements spécifiques et celles qui dépendent des procédures. Cela ne devrait pas générer de surcharge de travail déraisonnable pour les opérateurs. Avis favorable.

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

Amendement CS199 de M. Aurélien Lopez-Liguori

M. Emeric Salmon (RN). L'amendement vise à rendre obligatoire la consultation de l'autorité administrative par les OIV sur le point d'accorder une autorisation d'accès à leurs points d'importance vitale – rien ne les y oblige aujourd'hui. En effet, il n'est pas anodin de mettre entre les mains d'un individu la clé d'infrastructures essentielles pour la nation.

Mme Catherine Hervieu, rapporteure. La faculté ouverte aux OIV de demander un avis à l'autorité administrative est bien appréhendée par les opérateurs. En actant le passage à une logique d'avis conforme et en élargissant aux accès à distance, le projet de loi renforce déjà les contrôles portant sur les accès aux sites sensibles. Il serait donc contre-productif d'imposer aux opérateurs de demander un avis à l'autorité administrative. Cela pourrait créer un encombrement déraisonnable des services chargés des enquêtes. Les administrations que j'ai auditionnées ont indiqué qu'elles travaillaient en bonne intelligence avec les OIV. Des relations de confiance sont en train de s'établir et, même s'il ne faut pas être naïf en la matière, une telle disposition ne serait sans doute pas conforme à l'esprit de la directive ni à l'urgence de la transposer et à la nécessité de la rendre efficace.

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

Amendement CS127 de Mme Catherine Hervieu

Mme Catherine Hervieu, rapporteure. Rédactionnel. Il s'agit de corriger une erreur de renvoi.

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

Amendements identiques CS481 de M. Éric Bothorel, CS43 de M. Arnaud Saint-Martin, CS140 de M. Édouard Bénard et CS169 de Mme Sabrina Sebaihi

M. Arnaud Saint-Martin (LFI-NFP). Il est proposé que le décret d'application encadrant les enquêtes administratives de sécurité pour l'accès aux points et aux systèmes d'information d'importance vitale soit pris après avis de la Cnil. Cela permettrait de motiver davantage les demandes d'enquêtes administratives, qui peuvent entraîner la consultation de données personnelles à caractère sensible.

Mme Sabrina Sebaihi (EcoS). Les enquêtes administratives de sécurité qui conditionnent l'accès à des infrastructures critiques peuvent nécessiter la consultation de casiers judiciaires et l'exploitation de traitements automatisés de données personnelles. Autrement dit, cela touche directement aux libertés individuelles, raison pour laquelle nous proposons cet amendement.

Mme Catherine Hervieu, rapporteure. Il est important que la Cnil puisse éclairer le gouvernement sur la protection des données privées et l'accès à des informations sensibles. Avis favorable.

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

Amendement CS200 de M. Aurélien Lopez-Liguori

M. Emeric Salmon (RN). Cet amendement vise à obliger les OIV à consulter l'autorité administrative lorsqu'ils envisagent de recruter une personne pour un poste où elle aura accès aux points d'importance vitale.

Il complète donc l'amendement CS199. La rapporteure avait estimé que ce dernier n'était pas conforme à la directive mais, si l'on ne rend pas obligatoire la consultation de l'autorité administrative, on crée une passoire car il n'y aura pas réellement de filtrage.

Mme Catherine Hervieu, rapporteure. Permettez-moi de relever qu'à l'occasion d'autres débats, votre groupe avait défendu avec vigueur la simplification administrative.

Les opérateurs sont déjà familiarisés avec le dispositif actuel. Ils sont très conscients de la nécessité d'être vigilants en matière de recrutement et savent quels sont les postes qui supposent de demander l'avis de l'autorité administrative.

Encore une fois, on progresse, avec la conscience partagée de la nécessité d'être extrêmement efficaces pour aboutir à des procédures qui protègent contre les cyberattaques et les ingérences. Votre amendement serait donc contre-productif. Il

ne correspond pas à l'esprit de ce texte, très attendu par les opérateurs et qui doit être opérationnel. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). Si les entreprises ont déjà l'habitude de solliciter l'avis de l'autorité administrative, c'est bien qu'elles y ont très largement recours. Rendre cette consultation obligatoire n'entraînerait aucun engorgement, d'autant que cela reste un avis consultatif.

Mme Catherine Hervieu, rapporteure. Votre amendement conduirait à un encombrement déraisonnable des dossiers à traiter par les services chargés des enquêtes, ce qui ne correspond pas à ce que vous souhaitez.

On sait que la transposition de la directive va augmenter le nombre d'OIV. L'acculturation prévue par le projet constitue déjà une étape.

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

Amendement CS201 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Le texte prévoit que la Commission européenne puisse intervenir en effectuant des missions de conseil auprès de nos OIV, lorsque ceux-ci sont considérés comme d'importance européenne.

Nous comprenons l'intention, qui consiste à renforcer la coordination et la sécurité collective au sein de l'Union. Mais, même encadrée, cette disposition soulève des questions de principe. Quelle est la légitimité de la Commission européenne pour diligenter des opérations de conseil dans nos OIV, qui plus est lorsqu'ils interviennent dans des domaines qui relèvent des compétences exclusives des États et qu'ils sont essentiels dans le quotidien des Français et pour notre indépendance – hôpitaux, réseaux d'énergie ou de communications, administrations ?

Nous voulons ouvrir le débat car nous pensons qu'il n'appartient pas à la Commission européenne, organe non élu, de diligenter des missions de conseil et, potentiellement, de collecter des données confidentielles sur nos OIV. C'est pourquoi nous proposons de supprimer ce mécanisme.

Mme Catherine Hervieu, rapporteure. Il convient tout d'abord de rappeler que si la directive a été proposée par la Commission, elle a été adoptée par le Parlement et par le Conseil.

Comme cela est indiqué dans la directive, les entités critiques d'importance européenne particulière sont les OIV qui fournissent des services essentiels similaires dans au moins six États membres. Il est bien entendu indispensable de transposer cette notion en droit national et j'aurai un avis défavorable. Néanmoins, je vais revenir sur les points que vous avez soulevés.

Les obligations imposées à ces entités sont en réalité peu contraignantes. Il s'agit d'accorder un accès en cas de mission de conseil de la Commission pour les

aider à se conformer à leurs obligations et à transmettre des informations supplémentaires à la Commission, si nécessaire.

L'objectif est avant tout d'assurer un recensement des entités critiques transfrontalières. Comme les dernières crises environnementales et les conflits l'ont montré, les risques pour la nation sont d'abord transfrontaliers. Votre amendement ferait peser de graves dangers sur le fonctionnement de l'économie comme de la société. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). Une nouvelle délégation de compétence dans un domaine qui relève exclusivement des États doit être votée à l'unanimité par le Conseil – ce qui n'est pas du tout le cas en l'occurrence. Même si l'on peut estimer que la question que nous soulevons est annexe, nous considérons qu'il n'est pas possible d'étendre les compétences de l'Union à la faveur d'une directive. Ce n'est pas notre conception de la souveraineté nationale.

Mme Catherine Hervieu, rapporteure. Les réseaux, qu'ils soient électriques ou ferroviaires, font partie des OIV. Ils ne s'arrêtent pas aux frontières de chacun des pays européens. Il faut donc être cohérent.

Mme Marina Ferrari (Dem). L'amendement vise à supprimer un alinéa qui permet à la Commission d'accéder à des informations concernant des OIV lorsqu'ils fournissent des services essentiels dans au moins six pays – c'est-à-dire lorsqu'il existe un risque collectif. Il est donc nécessaire de maintenir cette disposition, car nous pouvons être interdépendants dans certains domaines.

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

*Suivant l'avis de la rapporteure, la commission **rejette** successivement les amendements CS202 et CS203 de M. Aurélien Lopez-Liguori.*

Amendement CS204 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Cet article prévoit que certains secteurs extrêmement souverains – comme la défense, le nucléaire ou la sécurité civile – peuvent être exclus du dispositif. Mais il s'agit seulement d'une faculté, ce qui introduit une dangereuse ambiguïté pouvant conduire à des interprétations différentes selon les circonstances.

Pour nous, il n'y a pas à tergiverser : la défense, le nucléaire et la sécurité publique doivent être systématiquement exclus de ce dispositif. Nous proposons donc de verrouiller le cadre juridique, car la souveraineté dans le domaine régalien n'est pas négociable.

Mme Catherine Hervieu, rapporteure. Un décret en Conseil d'État précisera le champ des exemptions. Le SGDSN collabore activement avec les services de la Commission européenne pour identifier les remontées d'informations

pertinentes et celles qui doivent être proscrites pour garantir le secret de la défense nationale.

Il n'y a donc pas de raison que le législateur impose au gouvernement d'exempter les entités critiques d'importance européenne particulière de toutes leurs obligations.

Avis défavorable.

M. Éric Bothorel, rapporteur général. Avis défavorable également. Cet amendement est contraire à l'objectif de la directive, laquelle laisse une marge d'appréciation aux États. Une exclusion générale de certains secteurs viderait la directive de son sens.

M. Aurélien Lopez-Liguori (RN). La défense, le nucléaire et la sécurité publique sont les fondements de notre indépendance nationale. Ce ne sont pas des compétences partagées avec d'autres États membres mais bien des compétences exclusives des États.

Le texte permet déjà d'exclure, par décret, les activités précitées du champ du dispositif. Mais cette décision revient au législateur. Nous devons affirmer qu'il s'agit de compétences qui relèvent des États et non de l'Union européenne.

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

*Suivant l'avis du rapporteur général, elle **adopte** l'amendement rédactionnel CS128 de Mme Catherine Hervieu, rapporteure.*

*Suivant l'avis de la rapporteure, la commission **rejette** l'amendement CS205 de M. Aurélien Lopez-Liguori.*

Amendement CS206 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Les drones utilisés par l'État collectent des données parmi les plus sensibles. Si leur traitement est confié à des prestataires non européens, ces dernières se retrouveront *de facto* sous le régime de lois extraterritoriales, comme le Cloud Act (Clarifying Lawful Overseas Use of Data Act).

Je pense aussi et tout particulièrement aux lois sur le renseignement qui permettent aux autorités chinoises d'accéder aux informations sans même nous en informer. Ce risque n'est pas théorique : DJI (Da Jiang Innovation) a mis fin au blocage automatique des vols de ses drones dans les zones d'exclusion aérienne, ce qui permet de cartographier l'intégralité des zones sensibles aux États-Unis, en France et dans l'Union européenne. C'est un risque pour la France, mais aussi pour l'Europe.

Avec cet amendement, nous voulons imposer que les données soient traitées exclusivement par des entreprises européennes dont le capital est majoritairement

détenu par des Européens. C'est une mesure de souveraineté car il n'y a pas de sécurité nationale sans maîtrise totale de nos données.

Mme Catherine Hervieu, rapporteure. L'article auquel fait référence cet amendement existe déjà dans le code de la défense. Il est simplement renuméroté par le projet de loi, afin de mieux l'intégrer dans ledit code. Cet article autorise la captation d'images par les services de l'État pour sécuriser les points d'importance vitale.

L'amendement modifierait un dispositif qui fonctionne bien et qui ne nécessite pas d'instaurer une préférence européenne particulière. Les services de l'État font déjà appel à des sociétés nationales ou, au besoin, à des partenaires européens. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). Je comprends que l'on n'ait pas envie de surtransposer la directive. Mais, en dehors des débats sur la LPM (loi de programmation militaire), quand avons-nous pu discuter de cybersécurité au sein de cette assemblée ? Il me semble que cela n'a pas été le cas depuis la loi sur le renseignement, en 2015 – je n'étais pas encore député.

Ce texte est l'occasion aborder le sujet, à un moment où nous savons quels sont les risques géopolitiques, d'espionnage et liés à l'extraterritorialité. En tant que législateurs, nous devons saisir cette opportunité pour parler de souveraineté, d'indépendance et d'ingérence. La question est la suivante : comment faire en sorte que les entreprises européennes soient les seules à traiter ces données ? Une approche souveraine serait en soi extrêmement bénéfique, mais elle le serait aussi pour nos entreprises, qui auront des marchés. Je ne vois pas pourquoi nous nous en priverions.

M. Éric Bothorel, rapporteur général. Depuis huit ans, l'Assemblée s'est penchée sur les sujets relatifs au numérique en général, mais aussi, parfois, à la cybersécurité en particulier. Je pense notamment à la loi visant à sécuriser et à réguler l'espace numérique, dite Sren, qui comprenait des dispositions concernant le cloud. Le sujet des données a également souvent été abordé, notamment à l'occasion de textes relatifs à la santé. Nous avons adopté des dispositions pour sécuriser celles-ci – ce qui a contribué à la mise en place de la certification SecNumCloud.

Je ne peux pas laisser dire qu'il n'y a pas eu de travaux sur ces sujets à l'Assemblée, alors même que nous examinons un texte destiné à transposer les directives REC, NIS 2 et Dora. Qui plus est, certains groupes d'études travaillent de manière intense sur ces sujets. Les travaux de celui que vous présidez ne sont pas inutiles, monsieur Lopez-Liguori.

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

Amendement CS466 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Cet amendement de cohérence vise à soumettre l'ensemble des OIV aux obligations de notification d'incidents importants et de vulnérabilités critiques prévues à l'article 17.

Mme Catherine Hervieu, rapporteure. La précision est utile. Avis favorable.

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

Amendement CS49 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Cet amendement vise à étendre la protection dont disposent les lanceurs d'alerte aux agents chargés du contrôle des OIV. Les lanceurs d'alerte sont des vigies citoyennes qui participent à l'intérêt général en révélant des scandales liés à des violations d'une norme ou à des pratiques condamnables.

Les OIV sont par définition essentiels au bon fonctionnement de la société, des institutions et de l'économie. Une défaillance majeure de l'un d'entre eux pourrait avoir des conséquences extrêmement graves pour l'ensemble du pays.

Dans le cadre de leurs missions, les agents habilités à rechercher et à constater les manquements à l'article 1er peuvent être confrontés à de telles défaillances présentant un risque majeur pour l'intérêt général. Il est donc indispensable qu'ils puissent alerter l'opinion et les pouvoirs publics sans risquer des poursuites.

Mme Catherine Hervieu, rapporteure. Les agents habilités ont pour mission de constater les manquements des opérateurs et de les signaler, en vue d'une éventuelle saisine de la commission des sanctions.

Leur habilitation est stricte et leurs pouvoirs sont très larges. Ces prérogatives impliquent en contrepartie une discrétion absolue sur les faits dont ils ont connaissance, afin de protéger le secret de la défense nationale.

Étendre à ces agents les dispositions de loi Sapin 2 pourrait fragiliser l'ensemble du dispositif de sécurisation des activités d'importance vitale. La confiance entre les opérateurs et les agents habilités pourrait être rompue, avec des conséquences potentiellement graves sur l'accès de ces derniers aux informations.

Le dispositif de protection des lanceurs d'alerte concerne des circonstances exceptionnelles, lesquelles pourront être examinées par la justice au cas par cas. Avis défavorable.

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

Amendement CS451 de M. Philippe Latombe

M. le président Philippe Latombe. Cet amendement vise à intégrer au sein de la commission des sanctions un représentant du ministère chargé du secteur d'activité auquel appartient l'entité qui fait l'objet d'une procédure.

Historiquement, il revient aux ministères de désigner quels sont les OIV dans leur domaine de compétences. Il serait donc justifié qu'un représentant du ministère concerné participe aux débats de la commission, car il serait en mesure d'apporter à charge ou à décharge des éléments non techniques – relatifs aux politiques publiques, économiques ou sociaux – susceptibles d'influer sur sa décision.

Mme Catherine Hervieu, rapporteure. Chaque secteur d'importance vitale est supervisé par un ministre coordonnateur, lequel veille à l'application du dispositif dans les secteurs d'activité de son champ de compétences.

La commission des sanctions prévue par ce texte permettra quant à elle de sanctionner les manquements des opérateurs.

Par conséquent, il ne me semble pas judicieux que des représentants du ministère soient à la fois régulateurs et juges. Cela contreviendrait au principe de séparation des fonctions d'enquête et de sanction et remettrait en cause l'impartialité de la commission, laquelle doit être aussi indépendante que possible. Avis défavorable.

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

*Suivant l'avis de la rapporteure, elle **rejette** l'amendement CS44 de M. René Pilato.*

Amendement CS467 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Cet amendement vise à revenir au texte initial du gouvernement s'agissant des autorités chargées de nommer les membres de la commission des sanctions. Cette rédaction est justifiée par la nature et les missions de cette commission, qui aura à connaître de sujets très techniques et opérationnels, liés notamment à la sécurité des activités d'importance vitale et à la cybersécurité.

Il paraît dès lors paradoxal de confier au président de l'Assemblée nationale et à celui du Sénat le soin de procéder à de telles nominations.

Mme Catherine Hervieu, rapporteure. La modification adoptée par le Sénat renforce le contrôle du Parlement sur la commission des sanctions, sans pour autant politiser sa composition. Compte tenu des pouvoirs confiés à cette commission, il me semble utile que le Parlement désigne une partie des personnalités qualifiées. Avis défavorable.

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

En conséquence, l'amendement CS45 de M. Arnaud Saint-Martin ***tombe****.*

Suivant l'avis de la rapporteure, la commission ***rejette*** *l'amendement CS462 de M. Arnaud Saint-Martin.*

Amendements identiques CS479 de M. Éric Bothorel et CS99 de M. Laurent Mazaury

M. Laurent Mazaury (LIOT). Cet amendement vise à faire figurer explicitement le principe du contradictoire, élément fondamental des droits de la défense dans toutes les procédures. La commission des sanctions pourra en effet infliger des sanctions lourdes aux entreprises, avec des amendes pouvant s'élever à 2 % de leur chiffre d'affaires annuel mondial.

Mme Catherine Hervieu, rapporteure. L'amendement apporte une précision utile en inscrivant l'obligation de contradictoire dans la loi. Avis favorable.

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

Amendement CS532 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Cet amendement rédactionnel fait suite à l'amendement CS467.

Mme Catherine Hervieu, rapporteure. Avis défavorable.

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

Amendements identiques CS129 de Mme Catherine Hervieu et CS461 de M. Arnaud Saint-Martin, amendement CS470 de M. Éric Bothorel (discussion commune)

Mme Catherine Hervieu, rapporteure. Avec mon amendement je propose que le mandat des membres de la commission des sanctions ne soit pas renouvelable, alors que le texte prévoit qu'il peut être renouvelé une fois. Cela permettra de garantir l'impartialité de cette commission, car l'indépendance de ses membres ne pourra pas être contestée. Son autorité s'en trouvera renforcée.

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons modifier les modalités de désignation des membres de la commission des sanctions, afin de garantir son impartialité et son indépendance. Nous voulons également renforcer cette dernière en supprimant la possibilité pour l'exécutif de renouveler le mandat des membres de la commission. Le caractère désintéressé de ses décisions s'en trouvera renforcé.

M. Éric Bothorel, rapporteur général. L'amendement CS470 est rédactionnel.

Avis favorable aux amendements CS129 et CS461.

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

*En conséquence, l'amendement CS470 **tombe**.*

*Suivant l'avis de la rapporteure, la commission **adopte** l'amendement rédactionnel CS469 de M. Éric Bothorel, rapporteur général.*

Amendement CS20 de Mme Sabine Thillaye

Mme Sabine Thillaye (Dem). Je m'interroge sur l'opportunité d'exempter les administrations de l'État et ses établissements publics administratifs ainsi que les collectivités territoriales, leurs groupements et leurs établissements administratifs de sanctions en cas de manquement.

Je comprends que certains soient absolument opposés à mon amendement, mais le dispositif relatif aux sanctions comprend des garde-fous. La commission des sanctions statue par décision motivée. Elle ne peut pas se prononcer sans avoir entendu l'opérateur concerné ou son représentant. À défaut, il doit avoir été dûment convoqué. Enfin, le prononcé de sanctions n'est pas automatique.

D'autres États membres prévoient que leurs collectivités peuvent faire l'objet de sanctions. Ne faut-il pas faire de même dans le cas où certaines administrations ou collectivités feraient preuve d'une forme de négligence, faute d'avoir pris conscience de la nécessité de se protéger ?

Mme Catherine Hervieu, rapporteure. Cet amendement implique en réalité d'étudier séparément les conséquences pour l'Etat et les collectivités. D'une part, prévoir que l'État et ses établissements publics peuvent être sanctionnés n'emporterait que peu de conséquences effectives. Il s'agirait d'un mécanisme comptable. Les sanctions prononcées par la Cnil ne concernent pas l'État et ses établissements publics. Les réserves émises par le Conseil d'État portent d'ailleurs seulement sur les collectivités territoriales.

D'autre part, il est opportun de limiter les charges supplémentaires qui pourraient être imposées aux collectivités territoriales. Elles ne bénéficient d'aucune marge de manœuvre budgétaire en raison des missions qu'elles doivent assumer et de celles qu'elles exercent au nom de l'État.

Les spécificités des collectivités plaident pour une exonération du régime de sanctions, comme le prévoit le projet – étant entendu que ce texte comprend aussi des mesures de police administrative qui leur sont bien applicables. Avis défavorable.

*L'amendement est **retiré**.*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS130 de Mme Catherine Hervieu, rapporteure.*

Amendement CS58 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Cet amendement tend à renforcer le contrôle exercé par l'État sur les contrats de concession relatifs à la gestion d'infrastructures critiques. Dans un contexte de montée des tensions géopolitiques, de menaces hybrides et de dépendances stratégiques, il est essentiel de garantir la souveraineté de la France dans les secteurs les plus sensibles.

Cet objectif suppose une vigilance particulière à l'égard des modalités de sous-traitance, afin d'écarter tout acteur ou technologie susceptible de compromettre la sécurité, la continuité d'activité ou la confidentialité des données. Il implique aussi de favoriser les acteurs économiques basés en France, mesure qui permettrait de réduire les vulnérabilités de la France vis-à-vis d'acteurs économiques étrangers.

En imposant d'intégrer des clauses de sécurité dans ces contrats, l'amendement permet de préserver les intérêts fondamentaux de la nation, tout en favorisant une chaîne de sous-traitance compatible avec les exigences de loyauté, de transparence et d'autonomie stratégique. Il s'inscrit dans une démarche de consolidation de la résilience industrielle française et de protection de notre souveraineté économique.

Mme Catherine Hervieu, rapporteure. Le contrôle de l'autorité administrative est garanti, puisque les OIV devront l'informer avant de recourir aux régimes dérogatoires en matière de marchés publics et de contrats de concession. Les modalités seront prévues par des dispositions réglementaires.

Le dispositif prévu ne concerne pas l'État mais bien les OIV. Il est destiné à éviter qu'un acteur hostile remporte un contrat et menace une activité d'importance vitale. Avis défavorable.

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

Amendement CS103 de M. Antoine Villedieu

M. Emeric Salmon (RN). Certains opérateurs d'importance vitale – aéroports, ports, réseaux d'énergie et d'eau – passent des marchés qui touchent directement à la sécurité nationale. Pourtant, leur régime juridique n'est pas clairement aligné sur celui des marchés de défense, ce qui crée une zone grise. En pratique, un arbitrage politique compliqué est nécessaire pour écarter un prestataire extra-européen, par exemple un fournisseur chinois ayant une position dominante dans les systèmes de détection de bagages. Il manque un outil juridique clair pour protéger nos intérêts essentiels.

Nous proposons une solution simple : aligner explicitement le régime des marchés des OIV sur celui des marchés de défense ou de sécurité nationale. Cela permettra aux opérateurs de repousser de façon claire et légale des prestataires

étrangers qui présentent un risque pour nos données, notre souveraineté et notre sécurité.

Mme Catherine Hervieu, rapporteure. Le dispositif prévu par le projet de loi est plus adapté que celui des marchés de défense ou de sécurité, qui est plus général et vise davantage à protéger le secret de la défense nationale. Votre amendement contribuerait sans doute à affaiblir la sécurité des opérateurs, ce que nous ne souhaitons pas. Avis défavorable.

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

Amendement CS207 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Trop souvent, nos opérateurs d'importance vitale (OIV) confient leurs marchés les plus sensibles – sécurité des réseaux, systèmes de commandement, hébergement de données critiques – à des entreprises extra-européennes. Cela a deux conséquences : d'une part, une dépendance technologique, d'autre part, la soumission à des lois extraterritoriales comme le Cloud Act ou la loi sur le renseignement en Chine. L'histoire récente en a pourtant montré les dangers : des entreprises américaines bloquent du jour au lendemain l'accès à des technologies jugées stratégiques – M. Trump l'a évoqué dans une lettre aux Gafam il y a quelques mois – et des fournisseurs étrangers coupent l'approvisionnement en composés critiques. Qui peut croire que cela n'arrivera pas à la France ou à l'Union européenne ? Personne.

Nous souhaitons donc édicter un principe clair : dans les marchés stratégiques, la priorité doit être accordée aux entreprises européennes. C'est une question de bon sens. Viser la souveraineté, ce n'est pas se priver de l'efficacité : lorsque nous ne possédons pas une technologie, il faut bien entendu se tourner vers l'étranger. L'écosystème numérique français est très performant – revenant de Corée du Sud, je peux affirmer qu'il est bien meilleur que celui de ce pays. Il faut l'utiliser. Ce principe est doublement vertueux, puisqu'il aura pour effet de protéger notre souveraineté et de renforcer notre industrie nationale, qui compte déjà des champions en matière de cybersécurité. Nous affirmons une vérité simple : la sécurité nationale ne se sous-traite pas à l'étranger, elle se construit chez nous.

Mme Catherine Hervieu, rapporteure. Le projet de loi nous prémunit déjà contre le risque d'ingérence étrangère en évitant qu'un acteur hostile ne se porte candidat à des marchés publics ou à des contrats de concession, et, le cas échéant, remporte le contrat. L'introduction d'une clause de préférence européenne restreindrait la portée du dispositif tel qu'il est conçu : au-delà de la nationalité de l'entreprise, il vise à protéger les opérateurs de tous types d'entreprises hostiles étrangères. Avis défavorable.

M. Aurélien Lopez-Liguori (RN). M. Macron, M. Barrot et Mme Chappaz ont multiplié les déclarations sur la préférence européenne. Chaque fois qu'il est question de numérique, de défense et de stratégie, on invoque la nécessité de prioriser les marchés européens, d'appliquer un European Buy Act.

J'ose imaginer que votre position sera cohérente avec celle du président de la République.

Mme Marina Ferrari (Dem). Votre amendement n'est pas si contraignant que vous le dites, puisqu'il prévoit que les OIV « choisissent en priorité » des entreprises européennes. Il offre une possibilité sans rien imposer.

Le European Buy Act que nous appelons de nos vœux doit nécessairement être travaillé au niveau européen. Nous transposons ici une directive européenne : conformons-nous le plus possible à cette dernière, et avançons en parallèle sur les dispositions relatives aux marchés stratégiques.

M. Éric Bothorel, rapporteur général. Je ne peux pas laisser dire que nous ne serions pas cohérents avec les politiques volontaristes qui sont menées pour défendre notre souveraineté. Notre droit comporte des dispositions en ce sens – citons notamment le SecNumCloud. Je rejoins les arguments de la rapporteure et de Mme Ferrari : les dispositions que vous proposez n'ont pas leur place dans le projet de loi.

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

*Elle **adopte** l'article 1er **modifié**.*

CHAPITRE II
DISPOSITIONS DIVERSES

Article 2 (articles L. 1331-1, L. 2113-2, L. 2151-1, L. 2151-4, L. 2171-6, L. 2321-2-1, L. 2321-3 et L. 4231-6 du code de la défense ; article 226-3 du code pénal ; articles L. 33-1 et L. 33-14 du code des postes et des télécommunications électroniques ; article L. 1333-9 du code de la santé publique ; articles L. 223-2 et L. 223-8 du code de la sécurité intérieure ; article 15 de la loi n° 2006-961 du 1er août 2006 relative aux droits d'auteur et aux droits voisins) : *Actualisation de références législatives*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS131 de Mme Catherine Hervieu, rapporteure.*

*Elle **adopte** l'article 2 **modifié**.*

Article 3 (articles L. 6221-2, L. 6222-1, L. 6242-2 et L. 6312-3 [nouveaux] du code de la défense ; article 711-1 du code pénal ; articles L. 33-1, L. 33-15 et L. 34-14 du code des postes et des communications ; articles L. 285-1, L. 286-1, L. 287-1 et L. 288-1 du code de la sécurité intérieure) : *Dispositions relatives à l'outre-mer*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS132 de Mme Catherine Hervieu, rapporteure.*

*Elle **adopte** l'article 3 **modifié**.*

CHAPITRE III
DISPOSITIONS TRANSITOIRES

Article 4 : *Modalités d'entrée en vigueur du titre Ier*

*La commission **adopte** l'article 4 **non modifié**.*

TITRE II
CYBERSÉCURITÉ

CHAPITRE IER
DE L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Article 5 : *Missions et compétences de l'autorité nationale de sécurité des systèmes d'information*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS267 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS62 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons préciser les missions de l'Agence nationale de la sécurité des systèmes d'information (Anssi) en y intégrant la promotion de la cyberprotection et de la cyberhygiène ainsi que l'éducation aux bonnes pratiques numériques. À l'heure où notre société est toujours plus interconnectée, où les guerres sont hybrides et où les attaques cyber se multiplient, la technologie est devenue incontournable dès le plus jeune âge. Les moyens de l'Anssi doivent être renforcés afin qu'elle puisse assurer des missions pédagogiques en la matière.

La numérisation de l'économie et de nos modes de vie ayant un impact majeur sur nos sociétés, l'éducation aux bonnes pratiques et la lutte contre l'illectronisme sont des enjeux majeurs de politique publique qu'il convient de traiter comme tels en les inscrivant formellement dans la loi, tout en rappelant le rôle de l'État en matière de cyberprotection et de cyberhygiène.

Mme Anne Le Hénanff, rapporteure. Les jeunes étant des acteurs clés de la cyber-résilience de la nation, je suis favorable à votre amendement.

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

Amendement CS209 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Dans son rapport sur les cybermenaces publié en juin 2025, la Cour des comptes pointe une faiblesse majeure : la dispersion et le cloisonnement des analyses des menaces cyber. Des dizaines d'études sont produites par les ministères, les agences, les opérateurs publics et les cabinets privés, mais aucune consolidation n'en est réalisée ; de fait, nous avons une vision parcellaire de la menace cyber. Conformément aux recommandations de la Cour

des comptes, nous proposons que l'Anssi centralise et synthétise ces informations pour créer un véritable observatoire de la menace cyber.

Mme Anne Le Hénanff, rapporteure. Je comprends l'idée générale de votre amendement, mais je ne saisis pas bien les notions de centralisation et de synthétisation des études. Je vous propose de le retravailler en vue de la séance. Demande de retrait ; à défaut, avis défavorable.

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

Elle ***adopte*** *l'article 5* ***modifié****.*

Après l'article 5

Amendement CS475 de M. Éric Bothorel, amendements identiques CS472 de M. Philippe Latombe et CS208 de M. Aurélien Lopez-Liguori (discussion commune)

Mme Anne Le Hénanff, rapporteure. Je partage votre préoccupation quant à la cybersécurisation des collectivités territoriales – c'est justement l'objet de NIS 2. Toutefois, s'agissant de ces amendements comme de tous ceux qui, de mon point de vue, n'ont pas de lien avec NIS 2 ou qui constituent une surtransposition, ma position sera défavorable.

M. Éric Bothorel, rapporteur général. Je partage l'avis de la rapporteure sur les amendements identiques.

La commission ***adopte*** *l'amendement CS475.*

En conséquence, les amendements CS472 et CS208 ***tombent****.*

Amendement CS171 de Mme Sabrina Sebaihi

Mme Sabrina Sebaihi (EcoS). Lorsqu'une mairie, une école ou un hôpital sont frappés par une cyberattaque, les collectivités locales sont en première ligne : elles doivent protéger leurs services, leurs données et leurs citoyens. Bien souvent, elles n'en ont ni les moyens ni les compétences – beaucoup de petites communes n'ont aucun spécialiste cyber. Aussi proposons-nous que les collectivités puissent conclure des conventions de coopération afin de mutualiser leurs moyens, leurs expertises, leurs équipements et leur personnel. Plutôt que de demander à chacune d'inventer seule sa cybersécurité, renforçons la coopération territoriale et le tissu local. Grâce à ces conventions, les collectivités pourront partager un expert, accéder à des infrastructures sécurisées et s'appuyer sur les centres spécialisés régionaux. Il s'agira, non pas d'une charge nouvelle, mais d'un outil de résilience mis à leur disposition pour se protéger.

Mme Anne Le Hénanff, rapporteure. La mutualisation est essentielle. Cela dit, les collectivités locales, notamment les intercommunalités, ont déjà

vocation à mutualiser leurs moyens. Votre amendement constituerait donc une surtransposition. Avis défavorable.

M. Éric Bothorel, rapporteur général. Le plan communal de sauvegarde (PCS) est vivement encouragé pour toutes les communes, mais il n'est obligatoire que pour celles qui sont exposées à un risque particulier et pour les établissements publics de coopération intercommunale (EPCI) qui comptent une de ces communes – je vous renvoie à l'article L. 731-3 du code de la sécurité intérieure. Votre amendement ne s'appliquerait donc pas à l'ensemble des communes ; c'est pourquoi mon avis est défavorable.

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

Article 5 *bis* : *Stratégie nationale en matière de cybersécurité*

*Suivant l'avis du rapporteur général, la commission **adopte** successivement les amendements rédactionnels CS269 et CS270 de Mme Anne Le Hénanff, rapporteure.*

*En conséquence, les amendements CS483 de M. Éric Bothorel et CS268 de M. Philippe Latombe **tombent.***

Amendement CS271 de M. Philippe Latombe

M. le président Philippe Latombe. Il s'agit d'intégrer la notion de souveraineté numérique et d'autonomie stratégique numérique dans la stratégie nationale.

Mme Anne Le Hénanff, rapporteure. Avis favorable.

M. Aurélien Lopez-Liguori (RN). Je m'étonne que vous défendiez un amendement visant à introduire la souveraineté numérique dans la stratégie nationale, alors que tout à l'heure, vous vous êtes opposé au fait de définir cette même souveraineté numérique.

Qu'est-ce que la souveraineté numérique ? Si Google, entreprise américaine, a des activités établies en France auxquelles nous recourons, cela va-t-il dans le sens de la souveraineté numérique ? Doit-on plutôt se concentrer sur les entreprises qui ne sont pas soumises à l'extraterritorialité ? La moindre des choses est d'utiliser des mots qui ont une définition juridique ; sans cela, nous affaiblissons les principes dont nous nous réclamons.

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

*Suivant l'avis du rapporteur général, elle **adopte** successivement les amendements rédactionnels CS272, CS274 et CS275 de Mme Anne Le Hénanff, rapporteure.*

*En conséquence, l'amendement CS273 de M. Philippe Latombe **tombe.***

Amendement CS276 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Vu la multitude des acteurs cyber – je pense notamment au groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma), et aux centres de réponse aux incidents de sécurité informatique, les CSIRT –, il me semble nécessaire de clarifier le rôle et la mission de chacun. La lisibilité de la politique de cybersécurité de l'État passe par une clarification des compétences. Le rapport de la Cour des comptes du 16 juin 2025 recommande d'ailleurs de préciser le rôle, les compétences et l'articulation des différents acteurs de l'écosystème cyber.

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

Amendements CS277 de Mme Anne Le Hénanff, rédactionnel, et CS211 de M. Aurélien Lopez-Liguori (discussion commune)

M. Aurélien Lopez-Liguori (RN). La stratégie nationale de cybersécurité ne peut être élaborée uniquement à Paris mais doit être le reflet des réalités du terrain. Ce sont les élus locaux qui affrontent des attaques contre leur collectivité, les maires qui voient leur mairie paralysée, les présidents de département ou de région qui gèrent les attaques contre les collèges et les lycées. Nous souhaitons que les associations d'élus et les représentants des professionnels du secteur de la cybersécurité soient obligatoirement consultés dans l'élaboration de la stratégie nationale et du cadre de gouvernance.

Mme Anne Le Hénanff, rapporteure. Il est souhaitable que les associations d'élus et les représentants des professionnels du secteur soient consultés – ils ont d'ailleurs largement contribué à nourrir notre réflexion sur le projet de loi. Je suis donc favorable à l'amendement CS211.

M. le président Philippe Latombe. Votre amendement rédactionnel est incompatible avec celui de M. Lopez-Liguori, madame la rapporteure, puisqu'il supprime la référence à la gouvernance à l'alinéa 4.

Mme Anne Le Hénanff, rapporteure. Tout à fait mais celui-ci n'est que rédactionnel. Je m'en remets à la sagesse de la commission spéciale.

M. Éric Bothorel, rapporteur général. Je suis favorable à l'amendement CS277 et défavorable au CS211.

M. Aurélien Lopez-Liguori (RN). Vous devrez expliquer aux maires, aux présidents de département et de région et à l'écosystème cyber que vous refusez de les faire participer à la gouvernance ! Je n'en prends pas la responsabilité.

*La commission **adopte** l'amendement CS277.*

*En conséquence, l'amendement CS211 **tombe**.*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS278 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS214 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Nous ne gagnerons pas la bataille du cyberespace sans apporter un soutien massif à la recherche. Les menaces évoluent à une vitesse vertigineuse, l'IA générative produit des attaques par phishing indétectables et massives, la cryptographie post-quantique redessinera la sécurité des données et les deep fakes deviennent des armes de désinformation et de manipulation à grande échelle. Or l'article 5 bis ne mentionne à aucun moment la recherche. C'est une lacune majeure que notre amendement vise à combler en mentionnant explicitement le soutien à la recherche en cybersécurité : laboratoires publics, universités, start-up qui engagent des innovations technologiques de rupture. Il y va de notre souveraineté : sans avance scientifique, nous serons condamnés à acheter nos solutions à des entreprises étrangères, sous législation américaine ou chinoise, et à être une colonie numérique de ces pays. Il y va également de notre économie et de notre compétitivité : la cybersécurité est un secteur d'avenir, créateur d'emplois hautement qualifiés, dans lequel la France et l'Europe doivent être des leaders et non des suiveurs.

Mme Anne Le Hénanff, rapporteure. Une politique de cybersécurité ne saurait être envisagée sans associer l'écosystème de recherche. Avis favorable.

M. Éric Bothorel, rapporteur général. La stratégie doit s'adapter de façon efficace et agile à une menace technologique et géopolitique spécifique et évolutive ; les priorités peuvent varier. Il faut donc se garder d'inscrire dans le dur des éléments qui figeraient notre politique de cybersécurité. C'est pourquoi je suis défavorable à cet amendement, comme à tous ceux qui tendent à ajouter à l'article 5 bis des dispositions détaillées ne relevant pas du niveau stratégique : plans divers, conditions de recours à des solutions techniques extra-européennes, etc. Ces sujets peuvent être déclinés en mesures sectorielles ou être traités dans le cadre du dialogue de très bonne tenue qu'entretiennent le gouvernement et le Parlement s'agissant de la cybersécurité, par exemple par le biais des questionnaires budgétaires.

M. Aurélien Lopez-Liguori (RN). Je comprends que l'on veuille donner de la souplesse à la stratégie de cybersécurité et qu'il faille éviter d'inscrire dans le marbre des principes qui pourraient changer demain. Or mon amendement traite du soutien à la recherche en cybersécurité, qui est une composante centrale de cette stratégie ; il fixe de surcroît un objectif non contraignant. Je ne comprends donc pas votre position.

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

*Suivant l'avis du rapporteur général, elle **adopte** l'amendement rédactionnel CS280 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS279 de M. Philippe Latombe

M. le président Philippe Latombe. À l'alinéa 5, il s'agit de mentionner la dépendance numérique parmi les risques liés à la cybersécurité. Pour illustrer cette menace, songeons au *kill switch* brandi par les États-Unis en réaction aux décisions de la Cour pénale internationale (CPI) ou à l'augmentation massive du prix de la licence VMware. Notez aussi qu'en réaction à l'amende infligée par la Commission européenne à Google il y a quelques jours, les États-Unis menacent d'appliquer une taxe sur tous les services numériques importés depuis leur territoire – licences et logiciels de Microsoft, Google ou autres. Nous devons intégrer le risque de dépendance à ces services.

Mme Anne Le Hénanff, rapporteure. Avis favorable.

M. Éric Bothorel, rapporteur général. La dépendance numérique est certes un sujet d'attention majeur, mais la directive traite de la cybersécurité. Si la souveraineté numérique et la cybersécurité sont corrélées, elles restent deux objets distincts caractérisés par un périmètre, une gouvernance et des acteurs propres. Pour ces raisons, je demande le retrait de l'amendement ; à défaut, j'émettrai un avis défavorable.

M. Aurélien Lopez-Liguori (RN). La souveraineté numérique et la cybersécurité sont au contraire totalement liées : l'une ne peut pas aller sans l'autre. Ce texte nous offre l'occasion unique d'introduire dans notre stratégie un principe absent de notre droit, la souveraineté numérique. Ne ratons pas le coche.

M. Vincent Thiébaut (HOR). Je ne comprends pas très bien votre raisonnement. Il me semble assez simple de définir la souveraineté numérique : il s'agit de notre capacité à faire appliquer nos lois et nos règles dans le monde virtuel par l'ensemble des acteurs du numérique, qu'ils soient français ou non, européens ou non. Quant à la dépendance numérique, comment la situez-vous ? Par rapport à la gouvernance d'internet ? De toute façon, nous sommes dépendants puisque nous ne fabriquons ni antennes ni infrastructures – ces dernières sont produites par des fabricants européens, pas par des fabricants français. Si je comprends votre préoccupation, je pense qu'il nous reste à mener une vraie réflexion pour pouvoir aboutir à une définition juridique.

Mme Anne Le Hénanff, rapporteure. Rappelons que cet article 5 *bis*, ajouté par les sénateurs, avait pour objectif de définir une stratégie nationale cyber, de grands principes généraux. Nous ne ferions pas de la surtransposition en adoptant cet amendement auquel je suis favorable.

M. Éric Bothorel, rapporteur général. Je n'ai d'ailleurs pas utilisé l'argument de la surtransposition pour demander le rejet de cet amendement. Il me semble qu'il y a une confusion entre souveraineté et cybersécurité. Il ne peut pas y avoir de cybersécurité sans souveraineté, dites-vous. Or nous n'avons jamais adopté une définition commune de la souveraineté. Dans cette salle, certains considèrent que l'Europe est un ennemi, tandis que d'autres sont pro-européens. Dès lors,

comment évaluer la dépendance concernant des technologies fabriquées avec des partenaires allemands, espagnols ou italiens ? Dans ce contexte, je préfèrerais éviter d'entrer dans ces considérations de dépendances, colonies ou souveraineté numériques, même si certains sont en attente de débats et de réponses sur ces sujets. En faisant de tels ajouts, au détour de ce texte fondamental, sans prendre le temps de réfléchir à une définition commune, nous pourrions provoquer des conséquences non désirées sur notre écosystème où il existe aussi des coopérations et des partenariats avec des partenaires européens ou américains. D'où ma position concernant cet amendement et d'autres à venir.

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

Suivant l'avis du rapporteur général, la commission ***adopte*** *successivement les amendements rédactionnels CS281 et CS282 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS212 de M. Aurélien Lopez-Liguori.

M. Aurélien Lopez-Liguori (RN). La commande publique représente quelque 10 % de notre PIB, soit 187 milliards d'euros par an. Elle constitue donc un levier colossal pour orienter les choix technologiques et renforcer notre souveraineté, d'autant qu'1 euro de commande publique équivaut à 8 euros de subvention. Pourtant, ce levier reste largement sous-utilisé pour soutenir notre cybersécurité et faire émerger nos champions européens. Vous remarquerez qu'en matière de marchés publics, nous faisons systématiquement référence à des fournisseurs français et européens : nous pensons que la souveraineté numérique se joue aussi au niveau européen et que notre écosystème numérique est européen. Nous constatons trop souvent l'attribution de marchés stratégiques à des entreprises soumises à des régimes juridiques extraterritoriaux tels que le Cloud Act américain. À un moment où nous essayons d'accroître le niveau de sécurité de nos opérateurs d'importance vitale et de nos infrastructures critiques, comment ne pas voir les dangers d'une telle pratique en matière de risques d'ingérence et de dépendance ? Nous écrivons donc noir sur blanc que la commande publique doit être intégrée dans une stratégie nationale de cybersécurité. C'est un objectif non contraignant – dans la ligne de ce que vous souhaitez au niveau européen avec l'European Buy Act – que vous n'avez aucune raison de refuser.

Mme Anne Le Hénanff, rapporteure. Partageant votre intérêt pour le sujet de la commande publique, j'ai suivi avec beaucoup d'attention les travaux de la commission d'enquête du Sénat, pilotée par Simon Uzenat. Dans le cadre des auditions que j'ai effectuées en tant que rapporteure du titre 2, nous avons d'ailleurs auditionné l'Ugap (Union des groupements d'achats publics). Toutefois, je vous propose de retirer votre amendement pour des raisons de rédaction et de positionnement dans le texte, et de le retravailler dans la perspective de l'examen en séance. À défaut, j'émettrais un avis défavorable.

M. Éric Bothorel, rapporteur général. Quand bien même cet amendement était retravaillé en vue de l'examen en séance, j'émettrais un avis défavorable : comme déjà indiqué, je voudrais éviter d'alourdir cet article 5 *bis*, que les ajouts portent sur la commande publique ou un autre sujet.

M. Aurélien Lopez-Liguori (RN). À vous entendre, il faudrait supprimer l'article 5 *bis*, celui-ci n'étant pas issu de la directive puisqu'il a été ajouté par les sénateurs. Si je comprends bien, on ne peut rien y ajouter et son existence-même pose problème.

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

*Suivant l'avis de la rapporteure, la commission **rejette** l'amendement CS213 de M. Aurélien Lopez-Liguori.*

Amendement CS182 de M. Vincent Thiébaut

M. Vincent Thiébaut (HOR). À un moment où des blocs internationaux lancent des campagnes de cyberattaques dans toute l'Union européenne, il nous semble pertinent d'indiquer que la stratégie nationale prend aussi en compte les perspectives de coopération européenne, ce qui est d'ailleurs prévu dans la directive NIS 2 et la directive sur la résilience des entités critiques. Une telle orientation est d'ailleurs cohérente avec le rapport annexé à la loi de programmation militaire 2024-2030, qui souligne que « la solidarité européenne dans le domaine de la cyberdéfense permet actuellement notamment les échanges de bonnes pratiques et l'assistance aux nations en difficulté et le partage d'informations ». D'où l'intérêt de cet amendement.

M. Éric Bothorel, rapporteur général. Dans la droite ligne de ce que j'ai déjà indiqué, j'émets un avis défavorable sur cet amendement.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS283 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS477 de M. Éric Bothorel

M. Éric Bothorel, rapporteur général. Cet amendement me permet de mentionner le travail effectué par le groupement d'intérêt public Action contre la cybercriminalité (GIP Acyma) en matière de cybermalveillance.

Mme Anne Le Hénanff, rapporteure. Avis favorable.

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

Amendement CS64 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Il va dans le sens d'un amendement adopté précédemment. Il s'agit de s'assurer que la stratégie nationale de cybersécurité comprendra bien les missions de cyberprotection, de cyberhygiène et d'éducation aux bonnes pratiques numériques décrites plus haut. Ces mesures d'éducation et de sensibilisation citoyenne et populaire doivent être au cœur de la stratégie nationale de cybersécurité. Leur inscription dans la loi permettrait de les sanctuariser et de les ériger en priorité, afin de faire du numérique un bien commun émancipateur. Cela suppose évidemment d'accorder des moyens supplémentaires à l'école, à l'Anssi et à l'ensemble des services publics, afin de limiter le nombre de services publics accessibles en ligne pour assurer un accueil physique aux personnes les plus éloignées du numérique.

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

Amendement CS181 de M. Vincent Thiébaut

M. Vincent Thiébaut (HOR). Nous souhaitons ici envisager un soutien aux collectivités territoriales, notamment les plus petites, qui doivent se soumettre à la directive NIS 2 sans en avoir nécessairement les moyens. Ce soutien peut être financier pour permettre l'acquisition de systèmes, mais il peut aussi prendre la forme d'un accompagnement en matière d'expertise et de conseil. Nombre d'élus locaux, notamment dans les petites collectivités, se sentent démunis face à ces sujets très complexes.

M. Éric Bothorel, rapporteur général. Avis défavorable.

Mme Anne Le Hénanff, rapporteure. Les auditions des associations d'élus nous ont montré que le soutien financier aux collectivités est central. Je suis favorable à cet amendement dont je suis d'ailleurs cosignataire.

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

Amendement CS183 de M. Vincent Thiébaut

M. Vincent Thiébaut (HOR). Nous proposons de transposer directement une disposition prévue à l'article 7 de la directive NIS 2, qui invite les États membres à promouvoir la formation, l'éducation, la sensibilisation et la diffusion des bonnes pratiques en matière de cybersécurité. La Revue nationale stratégique 2025 souligne avec force que la résilience doit devenir un réflexe partagé par l'ensemble de la nation. Il est d'autant plus important de former les citoyens que le facteur humain est la première source de faiblesse en matière de cybersécurité.

M. Éric Bothorel, rapporteur général. Sagesse.

Mme Anne Le Hénanff, rapporteure. Avis favorable.

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

En conséquence, l'amendement CS284 de Mme Anne Le Hénanff, rapporteure ***tombe****.*

Amendement CS98 de M. Philippe Latombe

M. le président Philippe Latombe. Je propose d'ajouter un alinéa prévoyant « la création d'un fonds de soutien spécifiquement destiné à accompagner les collectivités territoriales et les établissements publics de coopération intercommunale à fiscalité propre qualifiés d'entités importantes ou essentielles n'ayant pas bénéficié du parcours de cybersécurité du plan France relance ».

Mme Anne Le Hénanff, rapporteure. Tout en comprenant l'intérêt de votre amendement, je suis défavorable à la création d'un tel fonds.

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

Amendement CS68 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Nous proposons l'intégration d'un volet territorial à la stratégie nationale de cybersécurité. Le gouvernement démissionnaire a drastiquement asséché financièrement les collectivités locales, surtout les collectivités rurales ou périurbaines, ce qui les a rendues vulnérables aux attaques cyber et aux dysfonctionnements. Elles demeurent sous-dotées en compétences, en ingénierie et en capacité de réponse. En l'absence d'une approche territorialisée et offensive en la matière, les inégalités d'accès au dispositif de protection et de formation risque de s'aggraver au détriment de la résilience collective. Il s'agit ici d'assurer le soutien des centres régionaux, de coordonner l'information, de renforcer les capacités locales, et aussi de faire de la cybersécurité une filière d'avenir accessible dans tous les bassins d'emploi.

Mme Anne Le Hénanff, rapporteure. Même si je comprends l'intérêt de votre amendement, je pense qu'il créerait une stratégie dans la stratégie et risquerait de conduire à un manque de lisibilité. Avis défavorable.

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

Amendement CS84 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Il vise à intégrer à la stratégie de l'Anssi le soutien technique et logistique à la création d'une filière de formation publique et nationale sur les métiers de la cybersécurité et de la cyberdéfense. En effet, il manque au moins 10 000 ingénieurs formés par an en France. Faute d'ingénieurs, seul un projet sur six en matière de cybersécurité est effectivement réalisé. La place des femmes dans ce type de filière est largement moindre : d'après une enquête réalisée en 2022 par l'Observatoire des métiers de la cybersécurité de l'Anssi, les formations en cybersécurité ne comprenaient que 14 % d'étudiantes. La France se prive de la moitié de sa matière grise. Aussi, il est essentiel pour l'État d'investir réellement dans une filière publique qui forme la population aux métiers

de cyber sécurité, qui soit accessible au plus grand nombre et diversifiée. L'Anssi pourrait ainsi apporter un soutien logistique et humain dans la constitution de programmes actualisés. Au vu de l'enjeu de souveraineté qu'elle représente, cette formation doit être administrée par des acteurs publics.

Mme Anne Le Hénanff, rapporteure. Avis favorable.

M. Éric Bothorel, rapporteur général. Cet amendement est satisfait : l'article 5 *bis* précise que les missions de l'Anssi incluent l'accompagnement et le soutien au développement de la filière cybersécurité en coordination avec les ministères compétents. On peut estimer que cela comprend la formation. Retrait ou avis défavorable.

M. Arnaud Saint-Martin (LFI-NFP). En le précisant, nous renforcerions cette orientation.

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

Amendement CS106 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Il vise à compléter la stratégie nationale de l'Anssi en y intégrant une étude sur le développement d'un système de stockage de données souverain, où les opérations, de l'hébergement à la gestion, seraient réalisées en France par le biais d'une entreprise française, sous juridiction française. En effet, la souveraineté numérique ne peut être garantie que par la maîtrise de l'ensemble de la chaîne : infrastructures matérielles, équipements, logiciels et gouvernance des données.

Le rapport de Bastien Lachaud et Alexandra Valetta-Ardisson sur la cyberdéfense souligne avec force l'impératif pour la France de disposer d'un espace de stockage souverain et sous juridiction nationale. Cette exigence de souveraineté est d'autant plus actuelle qu'un mégacentre de données dédié à l'intelligence artificielle doit prochainement s'implanter dans le village de Fouju, au nord de ma circonscription. Ce projet est financé en partie par le fonds émirien MGX. Une telle situation illustre concrètement les risques de dépendance stratégique, en exposant la France à une captation de ses données et à une mise en danger de sa souveraineté numérique.

Plus globalement, le groupe LFI estime que la stratégie nationale de cybersécurité ne saurait être pleinement efficiente que si les données stratégiques et sensibles sont gérées de manière souveraine, sous contrôle de l'État et exclusivement soumises à la juridiction française.

Mme Anne Le Hénanff, rapporteure. Pour avoir été corapporteure avec Frédéric Mathieu d'un rapport d'information sur les défis de la cyberdéfense, je comprends l'intérêt de votre proposition. Elle n'est cependant pas située au bon endroit puisqu'elle revient à faire une demande d'étude dans la stratégie. Je vous

propose donc de retirer votre amendement et de le retravailler dans la perspective de l'examen en séance publique. À défaut, j'émettrais un avis défavorable.

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

Amendement CS177 de Mme Véronique Riotton

Mme Véronique Riotton (EPR). Il vise à enrichir la stratégie nationale de cybersécurité en y intégrant explicitement la notion et les bonnes pratiques de la cyberhygiène. Pour reprendre la terminologie de la directive NIS 2, la cyberhygiène constitue le socle d'un cadre proactif de préparation et de sûreté globale. Concrètement, il s'agit d'intégrer des gestes simples et essentiels tels que les mises à jour régulières des logiciels et matériels, la gestion rigoureuse des accès utilisateur, ou encore la sauvegarde régulière des données critiques. Ces pratiques sont au cœur de la prévention et de la résilience face aux cybermenaces. La directive européenne et l'Enisa (Agence de l'Union européenne pour la cybersécurité) insistent sur ce point. Sans diffusion d'une véritable culture de cyberhygiène, nos infrastructures resteront fragiles. Cet amendement n'introduit pas de contraintes supplémentaires, mais tend à assurer la cohérence entre notre stratégie nationale et les exigences européennes, comme l'ont d'ailleurs fait la Belgique et l'Espagne. La cyberhygiène est complémentaire de la cybersécurité.

Mme Anne Le Hénanff, rapporteure. Pour les raisons précédemment évoquées, j'émets un avis favorable.

M. Éric Bothorel, rapporteur général. Votre demande est satisfaite par l'adoption de l'amendement CS64.

Mme Véronique Riotton (EPR). Je vérifierai la rédaction de cet amendement CS64. En attendant, je retire le mien.

*L'amendement est **retiré**.*

Amendement CS285 de M. Philippe Latombe

M. le président Philippe Latombe. Il a pour but d'inscrire dans la loi, après l'alinéa 9, le rôle stratégique du logiciel libre et des standards ouverts pour atteindre les objectifs de sécurité, de résilience et de souveraineté.

En matière de sécurité, la transparence du code source est une garantie essentielle de confiance en permettant l'auditabilité des solutions déployées sur nos infrastructures critiques. La directive NIS 2 souligne d'ailleurs en son considérant 52 : « Les politiques qui promeuvent l'introduction et l'utilisation durable d'outils de cybersécurité en sources ouvertes revêtent une importance particulière. » C'est bien dans le considérant, mais pas dans le texte de la transposition.

En matière de résilience, le recours aux standards ouverts et aux logiciels libres est le meilleur rempart contre le risque d'« enfermement propriétaire » – nous en avons parlé à propos de la dépendance technologique.

En matière de souveraineté numérique, promouvoir le logiciel libre revient à investir dans le développement de compétences nationales et européennes, à renforcer notre filière technologique, et à s'assurer que nos infrastructures critiques ne dépendent pas de technologies soumises à des législations extraterritoriales.

Mme Anne Le Hénanff, rapporteure. Votre proposition ne s'apparente pas à une surtransposition dans la mesure où elle se situe dans le cadre de l'article 5 *bis* qui porte sur la stratégie. C'est pourquoi j'émets un avis favorable.

M. Éric Bothorel, rapporteur général. Je suis très sensible à la promotion de l'utilisation des logiciels libres et des standards ouverts. Nous savons tous qu'une partie de la souveraineté et de la moindre dépendance dépend de l'interopérabilité, de la portabilité et de l'ouverture d'un certain nombre de logiciels. En cohérence avec la position que j'ai adoptée jusqu'à présent, je devrais émettre un avis défavorable. Comme l'amendement se rapporte à un sujet qui m'est cher, je vais m'en remettre à la sagesse de la commission.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS287 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS286 de M. Philippe Latombe

M. le président Philippe Latombe. En cohérence avec ce que nous avons fait à l'article 1er, je propose de compléter l'alinéa 10 par les mots : « et d'autonomie stratégique numérique ». Il s'agit de compléter le texte au titre de la directive NIS 2 et pas seulement au titre de la directive sur la résilience des entités critiques (REC).

Mme Anne Le Hénanff, rapporteure. Avis favorable.

M. Éric Bothorel, rapporteur général. Je l'ai déjà dit, mais j'aimerais vous convaincre d'être un peu raisonnables : à force d'ajouts dans cet article 5 *bis*, le texte va finir par manquer de clarté. Avis défavorable.,

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

Amendement CS210 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Il s'inspire d'un constat de la Cour des comptes : chaque ministère a ses propres systèmes, vulnérabilités et obligations, et en est à un stade différent du développement de sa doctrine cyber. Il en résulte une fragilité globale. La Cour des comptes recommande la déclinaison par ministère d'une stratégie nationale. C'est la seule manière d'assurer une appropriation réelle

et d'élever le niveau de sécurité des ministères tout en tenant compte des priorités et des structures de chacun d'entre eux.

Mme Anne Le Hénanff, rapporteure. L'idée est intéressante, mais une telle disposition alourdirait l'article. Avis défavorable.

M. Éric Bothorel, rapporteur général. Je ne pourrais pas dire mieux : cela alourdirait un article qui a déjà été beaucoup alourdi.

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

Amendement CS39 de Mme Sabine Thillaye

Mme Sabine Thillaye (Dem). Les PME peuvent se tourner vers une multitude d'acteurs publics comme l'Anssi, les CSIRT territoriaux, la plateforme Cybermalveillance et autres pour répondre aux menaces cyber. Dans un souci de clarté, j'aimerais que l'on mentionne la création d'un point de contact au niveau national ou régional, comme le prévoit directive NIS 2. Un décret pourrait préciser le nom de l'organisme qui assumera ce rôle.

Mme Anne Le Hénanff, rapporteure. La mise en œuvre de la loi va concerner toute une série d'acteurs, listés par l'Anssi, qui interviendront auprès des 15 000 entités. Ajouter une entité supplémentaire – centre d'appels ou contact national – réduirait la lisibilité du dispositif. C'est le rôle des CSIRT. Les PME et TPE peuvent se tourner vers les chambres des métiers et de l'artisanat, les chambres de commerce et d'industrie (CCI) et des organisations telles que le Medef ou la CPME. Avis défavorable

M. Éric Bothorel, rapporteur général. Merci de faire la publicité de la plateforme Cybermalveillance, le 17Cyber, forme d'hommage au travail des équipes de Jérôme Notin. C'est en quelque sorte le point de contact que vous demandez. Lancé il y a quelques mois et consacré en fin d'année dernière, c'est une des fiertés de notre pays. Votre demande est donc en grande partie satisfaite. Avis défavorable.

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

Amendement CS40 de Mme Sabine Thillaye

Mme Sabine Thillaye (Dem). Il s'agit, une fois encore, de répondre aux besoins spécifiques des PME, afin de les aider à répondre aux exigences que leur impose l'accroissement des menaces cyber, ce qui représente des coûts importants pour elles. Il me paraît important de préciser des modalités d'accompagnement.

Mme Anne Le Hénanff, rapporteure. L'idée est très intéressante mais il faut veiller à ne pas alourdir le texte d'autant que sera publié l'organigramme des acteurs qui accompagneront les 15 000 entités. Avis défavorable.

M. Éric Bothorel, rapporteur général. Même avis. J'apprécie de vous entendre dire que la charge est due à la menace d'être attaqué plus qu'à la mise en conformité pour tenter d'échapper aux attaques.

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

Amendement CS41 de Mme Sabine Thillaye

Mme Sabine Thillaye (Dem). Il est défendu.

Mme Anne Le Hénanff, rapporteure. Avis défavorable.

M. Éric Bothorel, rapporteur général. Cet amendement demande à inscrire un volet sur la gestion des vulnérabilités incluant la promotion et la facilitation de la divulgation coordonnée des vulnérabilités. Quitte à faire la promotion de ce qui existe, signalons le travail des CSIRT et du Cert (centre d'alerte et de réaction aux attaques informatiques).

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

Amendement CS100 de M. Laurent Mazaury

M. Laurent Mazaury (LIOT). Il s'agit certes d'un alourdissement, mais il est léger : l'ajout de sept mots. Je propose de prévoir un déploiement territorial de la nouvelle stratégie nationale en matière de cybersécurité, prévue à l'article 5 *bis*. En transposant la directive NIS 2, ce projet de loi fait le choix de soumettre les collectivités locales à de nouvelles exigences. Il est donc essentiel que la nouvelle stratégie de cybersécurité fasse l'objet d'un déploiement local adapté aux spécificités des territoires, notamment des territoires d'outre-mer. Cela permettra de donner de la visibilité aux élus locaux souvent éloignés des capacités d'agir, de clarifier les rôles de chacun, et surtout d'assurer la pérennisation de certains financements existants.

Mme Anne Le Hénanff, rapporteure. Pour être taquine, je dirais que votre demande est satisfaite dans la mesure où NIS 2 va concerner 15 000 entités, dont quelque 2 500 collectivités locales. Ce sont bien les territoires qui vont devoir se mettre en conformité avec la directive. Sous la tutelle de l'Anssi, la liste des intervenants sera déclinée de manière de plus en plus fine sur les territoires. Selon les territoires, ce sera un syndicat mixte du numérique, une agglomération ou une région. De fait, ce sera territorialisé. Avis défavorable.

M. Éric Bothorel, rapporteur général. Même si ce sont sept jolis mots, je suis de l'avis de Mme la rapporteure et je considère que le 5° *ter* de l'article prévoit les modalités d'accompagnement des collectivités territoriales par l'État, ce qui me semble satisfaire votre demande. Retrait ou avis défavorable.

M. Laurent Mazaury (LIOT). Comme cela concerne particulièrement nos territoires d'outre-mer, je vais maintenir mon amendement.

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

*Suivant l'avis du rapporteur général, la commission **adopte** successivement les amendements rédactionnels CS289 et CS290 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS288 de M. Philippe Latombe

M. le président Philippe Latombe. Au vu de vos précédentes interventions, monsieur le rapporteur général, je ne me fais guère d'illusion sur votre avis concernant cet amendement qui vise à intégrer les notions de souveraineté numérique et d'autonomie stratégique numérique dans la stratégie nationale.

M. Éric Bothorel, rapporteur général. En effet, ma position n'a pas changé : avis défavorable.

M. Aurélien Lopez-Liguori (RN). Alors que les États-Unis de Trump sont en train de renforcer le Cloud Act et d'expliquer aux Gafam que le déni de service peut être un instrument de guerre commerciale, alors la guerre est aux frontières de l'Europe, en Ukraine, et que des États comme la Corée du Nord et la Russie nous agressent au niveau cibler, nous avons réussi à ne pas ajouter la notion de souveraineté numérique dans l'article 5 *bis*. Je tenais à vous en féliciter.

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

Amendement CS215 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Une grande part de nos opérateurs d'importance vitale se reposent sur des technologies non européennes, soumises à des législations extraterritoriales – citons Microsoft Azure pour le Health Data Hub, Microsoft pour l'éducation nationale, Amazon pour certains services de l'État. Or chaque fois que nous choisissons une solution américaine ou chinoise, nous perdons un peu de notre autonomie. Cet amendement vise à intégrer dans le rapport un bilan de nos dépendances ainsi qu'une analyse des efforts de relocalisation engagés et de l'évolution du tissu industriel français et européen. Cela apporterait de la transparence à nos concitoyens et renforcerait le contrôle démocratique exercé par le Parlement. La souveraineté numérique ne saurait se limiter à un principe, elle doit être une réalité vérifiable.

Mme Anne Le Hénanff, rapporteure. Le champ de votre amendement est trop vaste. Avis défavorable.

M. Éric Bothorel, rapporteur général. Pour d'autres raisons, avis défavorable.

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

*Elle **adopte** l'article 5* bis ***modifié***.

La réunion est suspendue de dix-neuf heures à dix-neuf heures dix.

CHAPITRE II
DE LA CYBER-RÉSILIENCE

Section 1
Définitions

Article 6 : *Définitions*

Amendements identiques CS484 de M. Éric Bothorel et CS266 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Il s'agit d'apporter une clarification au sujet des agents soumis aux dispositions du présent projet de loi en précisant la définition de l'agent agissant pour le compte des bureaux d'enregistrement. Celle-ci vise notamment à dresser une liste non exhaustive incluant les revendeurs de noms de domaine ainsi que les fournisseurs de services d'anonymisation ou d'enregistrement fiduciaire, comme le prévoit la directive.

M. Éric Bothorel, rapporteur général. La présentation de ces amendements est pour moi l'occasion de remercier Anne Le Hénanff et les rapporteurs sur les autres parties du texte pour le travail qu'ils ont fourni tout au long de l'été.

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

*Suivant l'avis du rapporteur général, la commission **adopte** successivement les amendements rédactionnels CS291 et CS292 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS485 de M. Éric Bothorel et CS294 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Pour clarifier et simplifier la rédaction de cet article, il importe, d'une part, d'utiliser directement au sein du 5° les définitions prévues aux 1° et 2°, d'autre part, d'ajouter les agents agissant pour le compte de bureaux d'enregistrement dans la définition prévue dans ce même 5°.

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

Amendements CS293 de Mme Anne Le Hénanff et CS295 de M. Philippe Latombe (discussion commune)

Mme Anne Le Hénanff, rapporteure. Cet amendement propose de reprendre la définition de la résilience retenue à l'article 1er du projet de loi. Même

si cette notion ne figure pas dans la directive NIS 2, il me semble opportun de l'intégrer dans le projet de loi.

M. le président Philippe Latombe. Je vais retirer mon amendement au profit du vôtre, madame la rapporteure.

L'amendement CS295 est ***retiré****.*

Suivant l'avis favorable du rapporteur général, la commission ***adopte*** *l'amendement CS293.*

Suivant l'avis du rapporteur général, la commission ***adopte*** *l'amendement rédactionnel CS296 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS486 de M. Éric Bothorel, CS297 de Mme Anne Le Hénanff et CS149 de Mme Marina Ferrari

Mme Marina Ferrari (Dem). Il s'agit de revenir à la définition stricte de la notion de vulnérabilité, telle qu'elle a été posée dans le règlement européen d'octobre 2024 concernant les exigences de cybersécurité horizontales pour les produits comportant des éléments numériques.

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

Amendement CS298 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Cet amendement a pour objet d'intégrer à l'article 6 la définition de la notion de cybermenace en s'appuyant sur celle donnée dans le règlement européen d'avril 2019 relatif à l'Agence européenne de cybersécurité.

M. Éric Bothorel, rapporteur général. La Commission européenne est en train de procéder à une révision de ce règlement et nous ne pouvons anticiper les évolutions qui en résulteront. Je vous demanderai de bien vouloir retirer votre amendement.

L'amendement est ***retiré****.*

Amendement CS179 de Mme Marie Récalde

Mme Marie Récalde (SOC). Il vise à introduire la définition de l'approche « tous risques » telle qu'elle a été énoncée au considérant 79 de la directive NIS 2.

Mme Anne Le Hénanff, rapporteure. Introduire cette définition dans le projet de loi, qui ne mentionne pas cette notion, ne nous paraît pas présenter d'intérêt concret : on ne saurait figer l'acception de la notion de risque alors que les risques sont de nature évolutive.

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

*Elle **adopte** l'article 6 **modifié**.*

Section 2
Des exigences de sécurité des systèmes d'information

Article 7 : *Liste des secteurs d'activité hautement critiques et « critiques »*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS300 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS87 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons intégrer dans la liste des secteurs hautement critiques pour le fonctionnement de l'économie et de la société les câbles sous-marins et leurs opérateurs. Leur bon fonctionnement et leur sécurisation sont indispensables pour de nombreuses infrastructures stratégiques et pour la continuité des échanges à l'heure où plus de 95 % du trafic mondial des données de communication transite par ces réseaux. Ils revêtent un caractère vital pour la sécurité nationale et la souveraineté numérique.

Or ils ne sont que trop mal protégés face aux risques de sabotage physique et de cyberattaques et face aux menaces de guerre hybride, comme l'ont mis en évidence dès 2023 Aurélien Saintoul et Lysiane Métayer dans leur rapport d'information sur les fonds marins, qui a joué à un rôle précurseur dans la nationalisation d'Alcatel Submarine Networks (ASN), essentiel à notre souveraineté dans le domaine numérique.

Mme Anne Le Hénanff, rapporteure. Les câbles sous-marins sont certes centraux dans la cybersécurité mais tout ajout à la liste des secteurs critiques et hautement critiques figurant en annexe de la directive NIS 2 et que le projet de loi reprend textuellement, constitue une surtransposition.

M. Éric Bothorel, rapporteur général. Votre amendement est satisfait : ces opérateurs sont déjà couverts par l'alinéa 4 de l'article 8 et l'alinéa 3 de l'article 9 du présent projet de loi. Certains relèvent en effet de la catégorie des opérateurs de communications électroniques telle qu'elle est définie au 15° de l'article L. 32 du code des postes et communications électroniques. Demande de retrait, sinon avis défavorable.

M. Arnaud Saint-Martin. J'ai été alerté par les opérateurs eux-mêmes sur la nécessité d'apporter une clarification sur cet enjeu stratégique majeur. Il importe d'être explicite. Je maintiens mon amendement.

M. Aurélien Lopez-Liguori (RN). L'argument de la surtransposition, si régulièrement mis en avant dans cette discussion, peut valoir quand un ajout nuit à la simplification ou affecte la concurrence entre pays membres, mais il ne saurait être utilisé lorsqu'il s'agit de protéger un secteur.

M. Éric Bothorel, rapporteur général. Je n'ai pas parlé de risque de surtransposition ; je me suis contenté de dire que l'amendement était satisfait.

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

Amendement CS73 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Au même titre que l'eau potable, les eaux usées, l'énergie, les transports, les télécommunications et la santé, l'alimentation doit figurer dans la catégorie des secteurs hautement critiques et non dans celle des secteurs critiques. Cette reconnaissance est essentielle pour garantir une protection adaptée, compte tenu des impératifs liés à la sécurité nationale, à la continuité des services essentiels et à la résilience collective face aux crises.

Mme Anne Le Hénanff, rapporteure. Défavorable pour les mêmes motifs que l'amendement précédent.

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

Amendement CS86 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin. Nouvelle tentative : je propose d'ajouter cette fois-ci l'enseignement supérieur à l'heure où les attaques dont il fait l'objet – pensons à celle subie Paris-Saclay –, les atteintes à sa liberté et à l'indépendance de ses étudiants se multiplient en France et partout dans le monde. Je déplore, par ailleurs, qu'un de nos amendements visant à établir un état des lieux des moyens dont disposent les universités pour faire face aux cyberattaques ait été déclaré irrecevable.

Mme Anne Le Hénanff, rapporteure. Ce serait là encore une surtransposition. Avis défavorable.

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

Amendement CS89 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Il s'agirait ici d'ajouter les satellites et leurs opérateurs. Les plateformes satellites, infrastructures essentielles dans le fonctionnement des systèmes d'information et de télécommunication, ont un intérêt stratégique majeur, qu'elles relèvent d'activités civiles, militaires ou duales.

Il est vraiment dommage qu'un de mes amendements demandant un rapport sur la vulnérabilité aux cyberattaques des satellites, plus particulièrement de leurs segments sol, ait été déclaré irrecevable alors qu'il s'agit d'un chantier majeur.

Mme Anne Le Hénanff, rapporteure. Défavorable.

M. Éric Bothorel, rapporteur général. Qu'il s'agisse de l'orbite terrestre basse ou du fond des océans, nous retrouvons les mêmes problèmes. Il est sans doute

urgent d'attendre que la Commission européenne achève ses travaux sur l'EU Space Act, qui prévoira des obligations pour les opérateurs en matière de cybersécurité.

M. Emeric Salmon (RN). Je me demande, monsieur Saint-Martin, si votre amendement n'est pas satisfait puisque dans l'article 7, l'espace figure déjà parmi les secteurs hautement critiques.

M. Arnaud Saint-Martin (LFI-NFP). Il me paraît utile d'être plus explicite. Mon amendement prend non seulement en compte les infrastructures en orbite, qu'elle soit basse, lointaine ou géostationnaire, mais aussi les segments sol.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS301 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS71 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Nous en venons à la liste des secteurs critiques et demandons que l'éducation en fasse partie, compte tenu des conséquences potentiellement dramatiques des cyberattaques sur les établissements et leurs élèves. Au risque de dresser un inventaire à la Prévert, il me paraît important de préciser le périmètre des secteurs à protéger.

Mme Anne Le Hénanff, rapporteure. Là encore, ce serait une surtransposition : avis défavorable.

M. Éric Bothorel, rapporteur général. Votre amendement me semble satisfait par l'alinéa 19 de l'article 8 et l'alinéa 6 de l'article 9 qui mentionnent les « établissements d'enseignement menant des activités de recherche » et les « établissements publics administratifs ».

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

*Elle **adopte** l'article 7 **modifié**.*

Article 8 : *Définition des entités essentielles*

Amendements identiques CS488 de M. Éric Bothorel et CS302 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Ces amendements visent à prendre en compte dans la loi 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 nationale.

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

Amendement CS79 de M. René Pilato

Mme Anne Le Hénanff, rapporteure. Le projet de loi se borne à décliner les seuils inscrits dans la directive : adopter votre amendement reviendrait à s'éloigner de ses stipulations.

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

Amendement CS13 de M. Denis Masséglia

M. Denis Masséglia (EPR). Cet amendement vise à supprimer une surtransposition.

Mme Anne Le Hénanff, rapporteure. Je comprends le sens de votre amendement mais j'émettrai un avis défavorable. Les articles 8 et 9 du projet de loi transposent strictement le champ d'application de la directive NIS 2 en précisant les seuils à partir desquels les entreprises sont considérées soit comme des entités essentielles, soit comme des entités importantes. Leur rédaction se fonde, conformément à l'article 2 de la directive, sur la recommandation 2003/361/CE de la Commission européenne qui définit les micro-entreprises, les petites entreprises et les moyennes entreprises. Comme la directive vise les grandes et moyennes entreprises, un principe de contraposition, par inversement des définitions, a dû être appliqué pour préciser le périmètre. La Belgique et l'Italie ont suivi la même logique de contraposition dans leurs lois de transposition. Ainsi dans la loi belge, une entreprise est considérée comme entité essentielle si elle a plus de cinquante employés ou si son bilan annuel ou son chiffre d'affaires annuel total excèdent 10 millions d'euros.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS303 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS78 de M. René Pilato

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

M. Éric Bothorel, rapporteur général. Défavorable également.

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

Amendement CS178 de Mme Véronique Riotton

Mme Véronique Riotton (EPR). Cet amendement vise à intégrer les éditeurs de logiciels dans le champ d'application de la directive NIS 2 afin qu'ils soient soumis aux mêmes obligations de sécurité que les fournisseurs de services numériques. Il s'agirait de leur imposer, dans une logique de responsabilisation, un socle minimal de sécurité dès le stade de la conception des logiciels et de permettre à l'Anssi d'exercer un contrôle en cas de faille critique. Il importe de protéger nos hôpitaux et nos entités essentielles.

Rappelons que dans les établissements de santé, de nombreux responsables de la sécurité des systèmes d'information (RSSI) alertent lorsqu'une faille est découverte dans un logiciel mais, comme rien n'oblige leurs éditeurs à publier rapidement un correctif, des cyberattaques sont susceptibles d'atteindre des systèmes vitaux pour la continuité des soins.

Mme Anne Le Hénanff, rapporteure. Avis défavorable : les éditeurs de logiciels sont inclus dans le projet de loi en tant qu'entreprises.

M. Éric Bothorel, rapporteur général. Pour ma part, madame la rapporteure, j'estime que l'on peut considérer cette question sous d'autres angles. Sagesse.

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

Amendement CS76 de M. René Pilato

Mme Anne Le Hénanff, rapporteure. En matière de collectivités territoriales, l'équilibre trouvé par le Sénat me semble être le bon et j'estime que votre amendement comme d'autres qui suivront risque d'altérer la résilience de la nation en matière de cybersécurité.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS304 de Mme Anne Le Hénanff, rapporteure.*

Amendement CS150 de Mme Marina Ferrari

Mme Marina Ferrari (Dem). Cet amendement vise à revenir à la rédaction initiale du texte en incluant à nouveau l'ensemble des communautés d'agglomération dans la catégorie des entités essentielles. Ces intercommunalités ont en effet comme compétence obligatoire de plein droit, en régie ou gestion directe, la gestion de l'eau potable et des eaux usées, activités considérées au titre de l'article 7 du projet de loi comme des secteurs hautement critiques pour le fonctionnement de l'économie et de la société.

Mme Anne Le Hénanff, rapporteure. Ce sera le seul amendement portant sur les seuils applicables aux collectivités territoriales auquel je donnerai un avis favorable. Il y va de l'égalité territoriale : je ne vois pas pourquoi seules les communautés d'agglomération comprenant une commune de plus de 30 000 habitants devraient être considérées comme entités essentielles. Cela dit, je le répète, l'équilibre trouvé par le Sénat me semble bon, s'agissant notamment des sanctions financières.

M. Éric Bothorel, rapporteur général. Avis favorable également.

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

Amendements identiques CS487 de M. Éric Bothorel et CS305 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. À la suite des auditions, il nous a paru nécessaire de faire figurer explicitement les établissements publics de santé et établissements et services sociaux et médico-sociaux parmi les entités essentielles afin de lever toute ambigüité même si le périmètre de la directive NIS 2 comprend la santé. Ces établissements ne partagent pas l'analyse de l'Anssi selon laquelle ils relèvent de la catégorie des entreprises, d'où ma proposition de les insérer explicitement dans le texte.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS306 de Mme Anne Le Hénanff, rapporteure.*

*Elle **adopte** l'article 8 **modifié**.*

Article 9 : *Définition des entités importantes*

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS307 de Mme Anne Le Hénanff, rapporteure.*

Amendements identiques CS490 de M. Éric Bothorel et CS308 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Ces amendements visent à prendre en compte au niveau de la loi 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 nationale.

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

Amendement CS151 de Mme Marina Ferrari

Mme Marina Ferrari (Dem). Il s'agit d'un amendement de coordination, tenant compte du retour à la rédaction initiale du projet de loi que nous avons adopté s'agissant des communautés d'agglomération.

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

*En conséquence, l'amendement CS74 de M. René Pilato **tombe**.*

Amendements CS180 de Mme Marie Récalde, amendements identiques CS105 de M. Antoine Villedieu et CS194 M. Laurent Mazaury, amendements identiques CS104 de M. Antoine Villedieu et CS193 M. Laurent Mazaury (discussion commune)

Mme Marie Récalde (SOC). Notre amendement CS180 vise à exclure du périmètre des entités importantes les communautés de communes dont la population regroupée est inférieure à 30 000 habitants. Même si les collectivités locales sont dans leur grande majorité soucieuses des questions de cybersécurité, il pourrait être compliqué pour les petites communautés de communes, pour la plupart situées en zone rurale, d'appliquer les nouvelles dispositions.

M. Emeric Salmon (RN). L'amendement CS105 et l'amendement de repli CS104 vont dans le même sens, avec des seuils respectifs de 30 000 et 20 000 habitants. Les communautés de communes de petite taille – dans ma circonscription, l'une d'elles n'excède pas 7 000 habitants pour trente-sept communes – ne disposent pas des services techniques et de l'ingénierie nécessaires.

Mme Anne Le Hénanff, rapporteure. L'avis est défavorable sur l'ensemble des amendements. Il ne faut pas laisser croire aux communes et aux EPCI que l'application de NIS 2 est facultative. Il s'agit certes d'un effort, mais les communes et les intercommunalités, même celles ne regroupant que 7 000 habitants, doivent commencer à réfléchir à la cybersécurité, laquelle vise à protéger les réseaux mais également les données, notamment personnelles et sensibles ainsi que celles collectées par l'échelon communal. Il faut éviter les inégalités de traitement et assurer la protection des données de tous les citoyens, que ceux-ci vivent dans une intercommunalité de 7 000 ou de 60 000 habitants.

M. Éric Bothorel, rapporteur général. Même avis.

M. Aurélien Lopez-Liguori (RN). Bien que cosignataire des amendements déposés par M. Antoine Villedieu, je n'en défends pas l'orientation. Je suis d'accord avec Mme la rapporteure : même si certaines communautés de communes éprouvent des difficultés à appliquer NIS 2, il serait discriminatoire que les données des Français habitant dans les zones rurales soient moins protégées. Une question technique subsiste toutefois, laquelle devrait nous amener à réfléchir, d'ici à la séance publique, à la création d'un mécanisme ou d'un fonds destiné à aider les petites communautés de communes pour assurer l'égalité de traitement des données.

Mme Marie Récalde (SOC). Les arguments de Mme la rapporteure sont parfaitement justifiés et comme nous avons adopté des amendements financiers créant notamment un fonds de dotation pour les petites communes, nous retirons notre amendement.

L'amendement CS180 est ***retiré****.*

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

Amendement CS75 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Il vise à mieux protéger le secteur de l'éducation face aux nouvelles menaces de cybersécurité.

L'école est une cible privilégiée des pirates informatiques pour plusieurs raisons. Tout d'abord, les établissements scolaires du second degré traitent beaucoup de données personnelles, dont le vol peut engendrer des conséquences dramatiques pour les personnes concernées. En outre, les infrastructures numériques des établissements scolaires sont, faute de budget suffisant, largement obsolètes, ce qui en fait des proies faciles. Cette situation, couplée à un manque de formation évident des personnels de l'éducation nationale découlant d'un manque de moyens et de temps, fait des établissements scolaires des cibles privilégiées.

L'inscription des établissements du second degré dans la catégorie des entités importantes renforcerait le niveau de leur protection, au bénéfice des élèves, des personnels de l'éducation nationale et du bon fonctionnement des collèges et des lycées.

Mme Anne Le Hénanff, rapporteure. Le sujet est important et il a toute sa place dans une stratégie globale, laquelle est exposée à l'article 5 *bis*. Les dispositions de l'article 9 sont au cœur de la directive, que nous surtransposerions en adoptant votre proposition. L'avis est donc défavorable.

M. Éric Bothorel, rapporteur général. Si vous souhaitiez retirer l'amendement en vue de le retravailler pour la séance publique, sachez que les établissements publics locaux d'enseignement sont, pour ceux placés sous la tutelle de l'État, des entités essentielles. Le gouvernement considère que l'intégration de ces établissements dans la catégorie des entités importantes affaiblirait le dispositif qui les concerne. En outre, leur système d'information leur est généralement fourni par les collectivités territoriales ou par le rectorat, lesquels font partie de cette catégorie. Je vous demande de retirer l'amendement, à défaut l'avis sera défavorable.

Mme Marina Ferrari (Dem). Les collèges et les lycées relèvent des départements et des régions, institutions couvertes par la directive NIS 2. La question peut se poser pour les petites communes : il conviendrait de réfléchir, en lien avec les intercommunalités, à des réponses opérationnelles aux problèmes relatifs aux équipements.

L'amendement est ***retiré****.*

Amendements identiques CS489 de M. Éric Bothorel et CS309 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Nous avons intégré tout à l'heure les établissements de santé, sociaux et médico-sociaux dans la catégorie des entités importantes : l'amendement vise à faire de même pour les entités essentielles.

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

Suivant l'avis du rapporteur général, la commission ***adopte*** *l'amendement rédactionnel CS310 de Mme Anne Le Hénanff, rapporteure.*

*La commission **adopte** l'article 9 **modifié**.*

Article 10 : *Autres entités susceptibles d'être désignées comme essentielles ou importantes par arrêté du premier ministre*

Amendement CS460 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise à introduire, après le mot « ministre » à l'alinéa 1 de l'article 10, les termes « après avis des ministères compétents des secteurs d'activité visés à l'article 7 de la présente loi. » L'objectif est double : apporter l'expertise des ministères coordonnateurs des secteurs d'activité visés par le projet de loi, afin que les listes d'entités importantes et essentielles prennent en compte les spécificités des écosystèmes concernés, et éviter d'oublier certaines entités.

Mme Anne Le Hénanff, rapporteure. L'avis des ministères compétents pourra utilement éclairer le processus d'élaboration de la liste des entités essentielles et de celle des entités importantes. L'avis est favorable.

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

*Suivant l'avis du rapporteur général, la commission **adopte** l'amendement rédactionnel CS312 de Mme Anne Le Hénanff, rapporteure.*

*Suivant l'avis de la rapporteure, la commission **adopte** les amendements identiques CS491 de M. Éric Bothorel et CS184 de M. Vincent Thiébaut.*

*La commission **adopte** l'article 10 **modifié**.*

Article 11 : *Compétence et territorialité des dispositions du titre II*

Amendement CS67 de M. René Pilato

M. Arnaud Saint-Martin (LFI-NFP). Il vise à supprimer la possibilité offerte aux fournisseurs de services numériques critiques établis hors de l'Union européenne de se soustraire à l'obligation d'établissement réel dans le territoire national en se limitant à la désignation d'un simple représentant local. Cette disposition est déconnectée de la réalité opérationnelle : elle ne garantit ni la maîtrise directe des infrastructures, ni la responsabilité pleine et entière de l'opérateur face aux exigences françaises. Elle peut par ailleurs être utilisée pour contourner les règles nationales et laisser certains acteurs dans l'orbite de législations extraterritoriales – l'exemple des États-Unis est bien connu.

La suppression de cette faculté est indispensable pour garantir l'obligation d'établissement effectif en France, condition *sine qua non* de l'exercice d'un contrôle robuste, transparent et efficient des acteurs numériques systémiques.

Mme Anne Le Hénanff, rapporteure. Je vois l'intérêt de l'amendement, néanmoins sa rédaction se heurte à un principe de réalité : la souveraineté nationale

est certes un enjeu important, mais la loi ne peut pas prévoir de critères aussi restrictifs. Je donne, presque à regret, un avis défavorable.

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

*La commission **adopte** l'article 11 **non modifié**.*

Article 12 : *Enregistrement des entités essentielles et importantes auprès de l'Anssi*

Amendement CS217 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). La directive prévoit une mise à jour tous les deux ans des listes des entités essentielles et importantes. Cette durée est une éternité dans le monde du numérique : des entreprises stratégiques apparaissent très régulièrement, d'autres disparaissent et les risques comme la menace évoluent sans cesse. Hier, les rançongiciels, aujourd'hui l'IA générative, demain, peut-être, l'informatique quantique, tous ces changements montrent qu'attendre deux ans pour ajuster la liste des entités à protéger revient à courir derrière le danger au lieu de l'anticiper.

Voilà pourquoi l'amendement vise à réduire le délai à un an. Cette mesure vise à faire preuve de réactivité pour protéger efficacement nos infrastructures dans un monde, celui du cyber, où le rythme des évolutions ne cesse de s'accélérer.

Mme Anne Le Hénanff, rapporteure. Une mise à jour annuelle me semble très restrictive et porteuse d'instabilité. L'avis est défavorable.

M. Aurélien Lopez-Liguori (RN). Nous nous mettons en danger. Peut-être qu'un État maîtrise l'informatique quantique et peut déjà déchiffrer l'ensemble des codes alphanumériques. Si ce n'est pas encore le cas, cela peut se produire dans un futur très proche. Attendre deux ans pour modifier la liste dans un tel contexte me semble totalement déraisonnable : une mise à jour annuelle est une mesure de sécurité.

M. Éric Bothorel, rapporteur général. Une compétition est engagée contre ceux qui nous menacent, mais si nous allions au bout de votre logique, même un délai d'un an serait trop long : si quelqu'un pouvait craquer les chiffrements, il ne serait pas tolérable d'attendre un an pour modifier les listes. La rédaction parfaite n'existe pas, donc nous suivons l'esprit et la lettre du texte de NIS 2 : revenir sur le délai fixé par la directive serait une surtransposition.

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

Amendements identiques CS492 de M. Éric Bothorel et CS314 de Mme Anne Le Hénanff

Mme Anne Le Hénanff, rapporteure. Le projet de loi emploie, en lieu et place des termes « entité fournissant des services d'enregistrement de noms de

domaine » utilisés dans la directive, l'appellation « bureau d'enregistrement », que l'on retrouve dans le code des postes et des communications électroniques.

L'amendement vise à garantir l'intégration des agents agissant pour le compte des bureaux d'enregistrement à la liste des entités établie par l'Agence nationale de la sécurité des systèmes d'information : cette disposition, conforme à NIS 2, adapte la terminologie entre la directive et le projet de loi.

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

Amendement CS313 de M. Philippe Latombe

M. le président Philippe Latombe. Il vise, par cohérence avec les dispositions que nous avons adoptées, à ce que la liste des entités essentielles et importantes soit la plus conforme possible à la réalité des secteurs d'activité concernés grâce à l'avis des ministères compétents. Les acteurs visés par le titre III sont notamment désignés par les ministères économiques et financiers : il serait opportun qu'il en soit de même dans le cadre de NIS 2.

Mme Anne Le Hénanff, rapporteure. Par cohérence, l'avis est favorable.

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

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

Amendement CS218 de M. Aurélien Lopez-Liguori

M. Aurélien Lopez-Liguori (RN). Le classement en entité essentielle ou importante crée des obligations lourdes de conformité, d'audit et de renforcement de la cybersécurité, pourtant le texte ne prévoit pas explicitement de notification aux entités de leur statut. L'amendement a pour objet de corriger cette lacune.

Mme Anne Le Hénanff, rapporteure. L'information me semble aller de soi et son inscription dans la loi n'est pas opportune : l'avis est défavorable.

M. Éric Bothorel, rapporteur général. L'amendement est partiellement satisfait par l'article L. 112-11 du code des relations entre le public et l'administration, lequel dispose que « Tout envoi à une administration par voie électronique ainsi que tout paiement opéré dans le cadre d'un téléservice (…) fait l'objet d'un accusé de réception électronique et, lorsque celui-ci n'est pas instantané, d'un accusé d'enregistrement électronique. » Un accusé de réception de l'enregistrement de l'entité sera donc délivré. L'avis est défavorable.

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

Amendement CS66 de M. Arnaud Saint-Martin

M. Arnaud Saint-Martin (LFI-NFP). Nous souhaitons réaffirmer l'importance de la protection des données sensibles, notamment celles à caractère personnel.

Autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (Cnil) joue un rôle de référence en matière de protection des données à caractère personnel contenues dans les fichiers et les traitements informatiques ou papier, aussi bien publics que privés. L'une de ses principales missions est de conseiller les pouvoirs publics en matière de conformité au droit existant en la matière : dans ce contexte, il nous semble indispensable de l'associer à l'élaboration du décret en Conseil d'État fixant les informations à transmettre par les entités essentielles, les entités importantes et les bureaux d'enregistrement, afin d'assurer la protection la plus élevée possible de leurs données personnelles.

Mme Anne Le Hénanff, rapporteure. Solliciter l'avis de la Cnil ne me semble pas utile. La rédaction du Sénat est suffisamment protectrice, donc l'avis est défavorable.

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

Amendement CS315 de M. Philippe Latombe

M. le président Philippe Latombe. Il s'agit d'un amendement d'appel visant à compléter l'article 12 par l'alinéa suivant : « Dans les trois ans après la promulgation de la présente loi, l'État identifie et sensibilise les entités concernées dans des conditions précisées par décret. » L'objectif est de se conformer aux annonces de l'Anssi sur les contrôles qu'elle effectuera, mais c'est davantage au gouvernement qu'aux rapporteurs qu'il revient de prendre cet engagement.

Mme Anne Le Hénanff, rapporteure. La directive prévoit un régime d'autodéclaration : l'amendement procède à une surtransposition, donc l'avis est défavorable.

M. Éric Bothorel, rapporteur général. Attendons la formation du nouveau gouvernement pour obtenir une réponse à votre proposition. L'avis est défavorable.

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

La commission ***adopte*** *l'article 12* ***modifié****.*

2. Réunion du mardi 9 septembre 2025, à 21 heures 30

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 1
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****.*

3. Réunion du mercredi 10 septembre 2025, à 14 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 Ier 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 1er, 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**.*

*En conséquence, la commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité vous demande d'**adopter** le projet de loi, adopté par le Sénat, relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (n° 1112) dans le texte figurant dans le document annexé au présent rapport.*