ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

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

Mardi 15 juillet 2025
Séance de 17 heures

Compte rendu n° 15

SESSION EXTRAORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

– Audition, ouverte à la presse, de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI). 2

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures trois.

La commission spéciale a procédé à l'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.

La séance est levée à dix-huit heures quarante.

Membres présents ou excusés

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

Réunion du mardi 15 juillet 2025 à 17 heures

Présents. - M. Éric Bothorel, M. Mickaël Bouloux, Mme Catherine Hervieu, M. Philippe Latombe, Mme Anne Le Hénanff, M. René Pilato, M. Vincent Thiébaut, Mme Sabine Thillaye

Excusé. - Mme Constance Le Grip