A S S E M B L É E N A T I O N A L E

17e LÉGISLATURE

Compte rendu

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

Mardi 9 septembre 2025
Séance de 15 heures

Compte rendu n° 16

SESSION EXTRAORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à quinze 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, M. Mickaël Bouloux, Mme Catherine Hervieu, Mme Anne Le Hénanff, 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.

La séance est levée à seize heures dix.

Membres présents ou excusés

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

Réunion du mardi 9 septembre 2025 à 15 heures

Présents. - M. Édouard Bénard, M. Éric Bothorel, M. Mickaël Bouloux, M. Jérôme Buisson, M. François Cormier-Bouligeon, Mme Virginie Duby-Muller, Mme Marina Ferrari, Mme Catherine Hervieu, M. Philippe Latombe, Mme Anne Le Hénanff, M. Aurélien Lopez-Liguori, M. Denis Masséglia, M. Emmanuel Maurel, M. Laurent Mazaury, M. Jacques Oberti, M. Stéphane Rambaud, Mme Marie Récalde, Mme Véronique Riotton, Mme Laetitia Saint-Paul, M. Arnaud Saint-Martin, M. Emeric Salmon, Mme Sabrina Sebaihi, Mme Liliana Tanguy, M. Vincent Thiébaut, Mme Sabine Thillaye