…le projet de loi relatif à résilience des infrastructures critiques et au renforcement de la cybersécurité

LA FRANCE TRANSPOSE 3 DIRECTIVES EUROPÉENNES POUR RENFORCER LA RÉSILIENCE ET LA CYBERSÉCURITÉ

Rapport n° 393 (2024-2025) de MM. Michel CANÉVET, Patrick CHAIZE et Hugues SAURY au nom de la commission spéciale présidée par M. Olivier CADIC.

Les attaques par rançongiciel ont augmenté de 30 % entre 2022 et 2023. **La cybermenace n'épargne plus aucun secteur de la vie économique et sociale** : 34 % de ces attaques visaient des TPE/PME, 24 % des collectivités territoriales, 10 % des entreprises stratégique, 10 % des établissements de santé et 9 % des établissements d'enseignement supérieur.

Ce phénomène a conduit l'Union européenne à adopter, en 2022, **trois directives**, pour lesquelles **le projet de loi relatif à résilience des infrastructures critiques et au renforcement de la cybersécurité prévoit la transposition** :

- la directive sur la **résilience des entités critiques** (REC) actualise le dispositif français de **sécurité des activités d'importance vitale**, augmentera de 2 à 6 les secteurs concernés et multipliera par 5 le nombre des opérateurs concernés de 300 à environ 1 500 ;

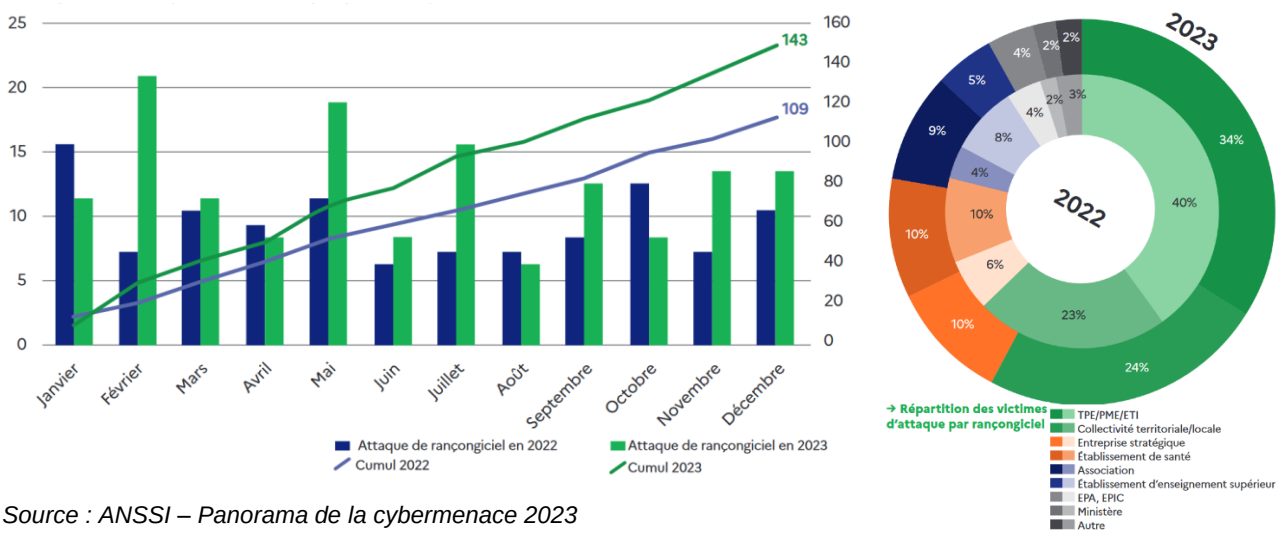
- la directive *Network and Information Security* (NIS 2), visant à **assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union**, va porter les 6 secteurs essentiels actuels à 18 secteur critiques et élargir le périmètre de régulation à 15 000 entités essentielles et importantes et près de 1 500 collectivités territoriales ;

- la directive *Digital Operational Resilence Act* (DORA) relative à la **résilience opérationnelle numérique du secteur financier, bancaire et assurantiel**.

***

La commission spéciale a adopté, le 4 mars 2024, le projet de loi relatif à résilience des infrastructures critiques et au renforcement de la cybersécurité. Le texte issu des débats de commission est enrichi de 61 amendements dont 53 de ses rapporteurs.

La montée de la cybermenace illustrée par les attaques de rançongiciels



Source : ANSSI – Panorama de la cybermenace 2023

1. TROIS DIRECTIVES EUROPÉENNES POUR RENFORCER LA RÉSILIENCE DES ENTITÉS CRITIQUES ET LA CYBERSÉCURITÉ

A. REC : LE PASSAGE D'UNE LOGIQUE DE PROTECTION À UNE APPROCHE DE RÉSILIENCE

Le titre I du projet de loi vise à transposer la directive (UE) 2022/2557 du parlement européen et du conseil du 14 décembre 2022 sur la résilience des entités critiques, dite « REC », en modifiant le code de la défense.

La directive REC, qui a été négociée sous présidence française de l'Union européenne, s'inspire en grande partie du dispositif français existant. Sa transposition en droit national consiste donc essentiellement en une actualisation du dispositif de sécurité des activités d'importance vitale (SAIV) en place depuis 2006.

Ce texte a pour ambition de fournir à l'ensemble des opérateurs du marché intérieur des standards de sécurité équivalents tout en offrant des règles de concurrence plus équitables.

Le Gouvernement a ainsi fait le choix de s'appuyer sur ce dispositif, en reprenant par exemple la terminologie existante, plutôt que de créer un dispositif ex nihilo. Cette décision semble opportune, le dispositif de SAIV étant désormais bien connu et maîtrisé par les opérateurs concernés. Par ailleurs, le nombre d'opérateurs d'importance vitale (OIV), qui est d'environ 300, ainsi que le nombre de points d'importance vitale, de l'ordre de 1 500, ne devraient pas évoluer de manière significative.

Toutefois, cette transposition marque un changement important de philosophie : elle acte **le passage d'une logique de protection des infrastructures d'importance vitale à une approche axée sur la résilience**.

Les obligations inscrites dans le projet de loi sont conformes à la directive

► Le champ d'application de la directive comprend 11 secteurs, contre 2 seulement antérieurement – énergie et transport – dans la directive de 2008. Concrètement, pour la France, la transposition de la directive REC se traduira par un élargissement du champ d'application du dispositif national actuel à plusieurs sous-secteurs, notamment les réseaux de chaleur et de froid, l'hydrogène et l'assainissement ;

► Le texte prévoit la réalisation d'un « plan de résilience opérateur », qui reprendra en partie le contenu des documents existants.

► Il impose également une obligation de notification des incidents et prévoit que les opérateurs désignés comme entités critiques d'importance européenne particulière, c'est-à-dire exerçant la même activité ou une activité similaire dans au moins six États membres, pourront faire l'objet d'une mission de conseil organisée par la Commission européenne ;

► Un mécanisme de sanction administrative pouvant être prononcée par une commission des sanctions créée à cet effet est prévu en cas de manquement. Ce dernier point posant la question des plafonds de sanction – 2 % du chiffre d'affaires ou 10 millions d'euros – inscrits qui, dans le projet de loi, sont plus élevés que dans d'autres États membres.

B. NIS 2 : UN CHANGEMENT DE PARADIGME POUR LES ENTITÉS ASSUJETTIES ET POUR L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Le titre II du projet de loi transpose la directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS2 ».

Ce texte conduit à un changement majeur de paradigme : il s'agit non plus seulement, comme avec la directive NIS 1, de sécuriser des infrastructures critiques (environ 500), mais aussi d'assurer la résilience quelque 15 000 entités « essentielles » ou « importantes », en tant

qu'organisations, et de l'ensemble de leurs systèmes d'information dans la lutte contre les cyberattaques (cf. encadré ci-dessous).

Principaux types de cyberattaques contre lesquelles entend lutter la directive NIS 2

► Les attaques par rançongiciel, qui consistent à exiger une rançon pour rendre des données ou ne pas les publier ;

► Les attaques par hameçonnage, qui visent les systèmes bancaires en ligne et les données financières des clients ;

► Les attaques sur Internet, exploitant les vulnérabilités des applications ;

► Les attaques de la chaîne d'approvisionnement, qui compromettent la sécurité d'une entité en exploitant les vulnérabilités des produits, services et systèmes de tiers (par exemple, un fournisseur de logiciels) ;

► Les attaques par déni de service distribué (DDoS), qui perturbent les transactions de grande valeur et le traitement des données ;

► Les attaques à caractère social, exploitant les vulnérabilités humaines.

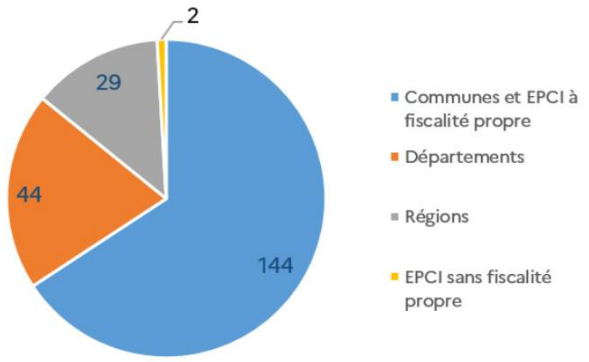
En outre, sur le constat étayé de l'augmentation des menaces cyber sur les collectivités territoriales (cf. grapique ci-dessous), le Gouvernement propose d'inclure dans la transposition près de 1 500 collectivités territoriales, groupements de collectivités et organismes placés sous leur tutelle, dont l'ensemble des régions et des départements, près de 1 000 communautés de communes et de 300 communes de plus de 30 000 habitants.

Pour la commission spéciale, **le choix d'inclure un grand nombre de collectivités territoriales et les établissements d'enseignement supérieur est ambitieux mais nécessaire**.

Nombre d'incidents cyber par type de collectivité en 2024

En 2024, l'ANSSI a traité 218 incidents cyber affectant les collectivités territoriales, soit une moyenne de 18 incidents par mois, dont 44 incidents affectant des départements et 29 incidents affectant des régions. Ces chiffres se révèlent élevés en comparaison du nombre de départements (101) et de régions (18).

Source : ANSSI – synthèse de la menace sur les collectivités territoriales en 2024



Les cyberattaques ont un coût très élevé, estimé en 2022 par le cabinet d'études économiques Asterès à 2 milliards d'euros.

Dans le secteur privé, une enquête menée en juin 2024 par l'ANSSI auprès des membres du CLUSIF, une association de professionnels de la cybersécurité, révèle qu'une cyberattaque coûte en moyenne 466 000 euros pour les TPE/PME, 13 millions d'euros pour les ETI et 135 millions d'euros pour les grandes entreprises.

Ce coût représente en moyenne 5 à 10 % du chiffre d'affaires de l'organisation, quels que soient sa taille ou son secteur d'activité, réparti entre les pertes d'exploitation (50 %), le coût des prestations externes d'accompagnement (20 %), le coût de remise en état et d'investissement dans le système d'information (20 %) et le coût réputationnel (10 %).

Dans la sphère publique, les établissements hospitaliers évoqués supra ont supporté des dégâts particulièrement importants : les coûts directs ont ainsi été estimés à 2,36 millions d'euros pour le Centre hospitalier Dax-Côte d'Argent (février 2021) et à plus de 5,5 millions d'euros pour le Centre hospitalier Sud-Francilien déjà cité.

Les collectivités territoriales et les intercommunalités ont également été lourdement affectées, avec des coûts directs estimés à 900 000 euros pour la Métropole Aix-Marseille-Provence (mars 2020) et à plus de 1,5 million d'euros pour la ville de Bondy (novembre 2020).

A ces coûts directs s'ajoutent des coûts indirects, liés aux activités non réalisées ou à la perte de confiances des usagers, mais leur chiffrage est complexe, tout particulièrement dans le cas des missions de service public.

L'adoption de la directive NIS 2 constitue une réponse à l'augmentation de la cybercriminalité

La directive NIS 2 distingue **deux catégories d'entités régulées : les entités « essentielles » et les entités « importantes »** du point de vue de la sécurité des systèmes d'information. Cette catégorisation s'établit selon leur degré de criticité, leur taille et leur chiffre d'affaires (pour les entreprises).

Deux caractéristiques qui conduisent à qualifier une **entité d'essentielle** :

- son appartenance à un secteur d'activité « hautement critique » ;
- le dépassement de certains seuils d'effectifs ou d'activité, à savoir le fait d'employer 250 personnes ou d'avoir un chiffre d'affaires annuel excédant 50 millions d'euros et un bilan annuel de plus de 43 millions d'euros.

Au total, selon l'ANSSI, quelque 2 000 entreprises privées devraient ainsi être considérées comme des entités « essentielles »

S'agissant des entités importantes, le texte prévoit que sont désignées comme telles les entreprises appartenant à un des secteurs d'activité « hautement critiques » ou « critiques » qui ne sont pas des entités « essentielles » et qui emploient au moins 50 personnes ou dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros.

Le tableau ci-dessous présente la classification des critères applicables aux entreprises selon qu'elles seront assujetties à l'une ou l'autre catégorie.

Seuils de classification des entités essentielles et importantes

Nombre d'employés	Chiffre d'affaires (millions d'euros)	Bilan annuel (millions d'euros)	Secteur d'activité hautement critique	Secteur d'activité critique
Supérieur à 250	Supérieur à 50	Supérieur à 43	Entités essentielles	Entités importantes
Entre 50 et 250	Compris entre 10 et 50	Compris entre 10 et 43	Entités importantes	Entités importantes
Inférieur à 50	Inférieur à 10	Inférieur à 10	Non concernées	Non concernées

La commission spéciale a néanmoins observé qu'une certaine incompréhension demeurait quant aux différences d'approche de la définition des seuils entre la directive (qui procède par exclusion) et le projet de loi qui définit positivement les critères d'assujettissement. **Un effort de pédagogie et de communication important devra être consacré à ce volet de l'application de la loi car dans en pratiques, les entités devront elles-mêmes identifier la catégorie dont elles relèvent.**

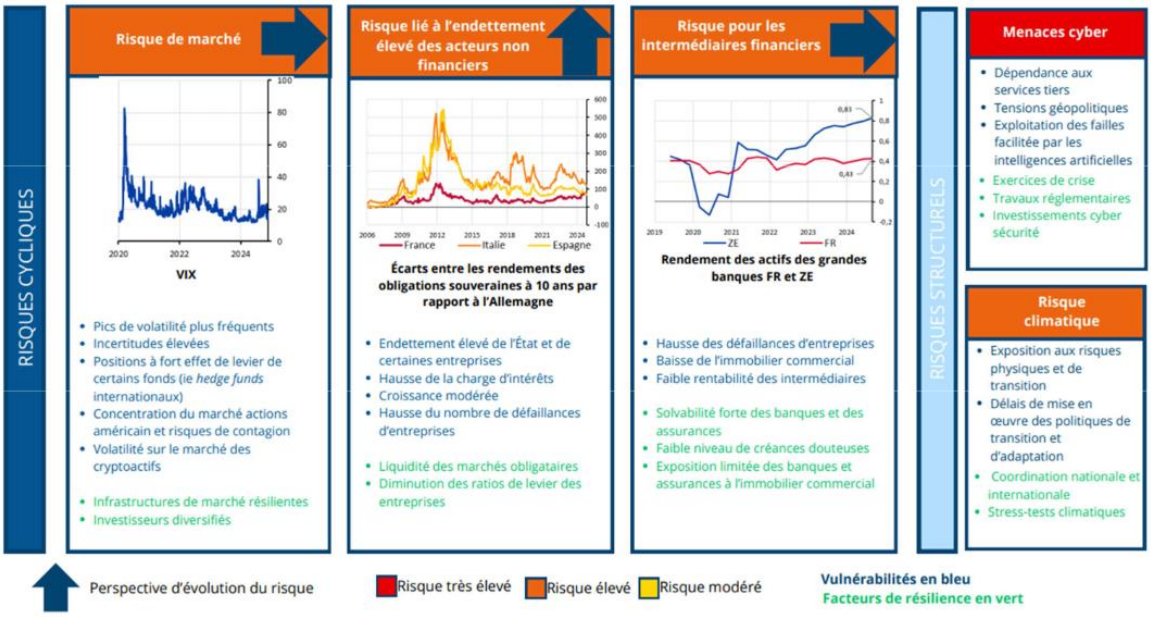
C. DORA : LES DISPOSITIONS SPÉCIFIQUES AUX SECTEURS FINANCIER, BANCAIRE ET ASSURANTIEL

Le titre III du projet de loi transpose dans le droit interne les dispositions de la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 en ce qui concerne la résilience opérationnelle numérique du secteur financier, dite « DORA ».

Ces dispositions viennent elles-mêmes modifier plusieurs directives encadrant les secteurs bancaire, financier et assurantiel pour prévoir que leur politique de gestion des risques liés aux technologies de l'information et de la communication est conforme au règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.

En effet, le secteur financier est une cible de choix pour les cyberattaques : il n'est que de rappeler la recapitalisation de la filiale américaine de la banque chinoise ICBC à hauteur de plusieurs milliards de dollars en 2024 du fait d'un rançongiciel. Par ailleurs, comme le souligne un rapport du comité européen du risque systémique (CERS) de 2020, le niveau élevé d'interconnexion dans le secteur financier, et notamment les interdépendances de leurs systèmes de technologies de l'information et de la communication (TIC), est susceptible de constituer une vulnérabilité systémique du fait d'une propagation possible d'un cyberincident de l'une des **22 000 entités financières** à l'ensemble du système financier. Ainsi que l'indique la direction générale du Trésor dans une étude sur le sujet, le risque cyber est en forte augmentation depuis plusieurs années . Dans son rapport sur la stabilité financière de décembre 2024, la Banque de France indique que le risque lié aux menaces cyber est très élevé, un niveau plus menaçant que le risque climatique, le risque de marché, le risqué lié à l'endettement des acteurs non financiers et le risque pour les intermédiaires financiers, qui n'est qu'élevé.

Évaluation des risques du système financier français en décembre 2024



Source : Banque de France, rapport sur la stabilité financière, décembre 2024

Selon l'Autorité des marchés financiers (AMF), les entités financières sont exposées à une large gamme de risques « TIC » : le déni de service sur l'infrastructure de trading, et donc plus globalement l'atteinte à la disponibilité de l'infrastructure de trading, l'atteinte à la confidentialité et l'intégrité des ordres, la compromission de l'algorithme de négociation (porte dérobée, code malveillant ou simplement présentant des bogues importés depuis des sources externes comme l'open source ou ChatGPT), ou encore l'atteinte à l'intégrité du Système d'Information (SI) supportant les services algorithmiques en vue de compromettre et modifier l'algorithme.

Au total, donc, **une réglementation plus rigoureuse que celle qui prévalait par le passé s'avère nécessaire**.

2. UN PROJET DE LOI ENFIN BIENVENU MAIS DONT LES MODALITÉS DE TRANSPOSITION NÉCESSITENT DES PRÉCISIONS

A. UNE TRANSPOSITION TARDIVE MAIS DONT PARADOXALEMENT LES PARTIES PRENANTES S'ESTIMENT PEU CONSULTÉES

La transposition de la directive NIS 2 devait intervenir avant le 17 octobre 2024 mais les circonstances politiques auront conduit à surmonter une dissolution de l'Assemblée nationale entre l'annonce du projet de loi initial pour juin 2024, le dépôt du texte le 15 octobre, puis une censure gouvernementale avant l'**audition de Mme Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique**, le 27 janvier 2025.

Au total, **la commission spéciale aura organisé sept réunions publiques entre le 17 décembre 2024 et le 11 février 2025** : deux auditions de responsables publics – outre la ministre précitée, M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et cinq tables rondes, avec les organisations professionnelles, des représentants des entreprises cyber, les associations d'élus, les autorités de régulation financière et des acteurs de la cyberdéfense. Cette séquence aura été la **contribution de la commission spéciale à une meilleure sensibilisation et à une meilleure information du public sur l'effort de résilience et de lutte contre les attaques cyber à engager**.

Paradoxalement, bien que **l'ANSSI** ait indiqué avoir conduit depuis septembre 2023 des **consultations avec plus de soixante-dix fédérations professionnelles, ainsi que les onze principales associations d'élus et quatre fédérations de collectivités territoriales** – et en dépit d'une étude d'impact faisant plus de 900 pages –, **l'ensemble des personnes entendues ont déploré un manque d'information et de concertation notamment sur les dispositions réglementaires d'application du projet de loi**.

B. LE RISQUE QUE LA SOUSTRANSPOSITION LÉGISLATIVE N'ENGENDRE UNE SURTRANSPOSITION RÉGLEMENTAIRE

Les points d'attention portés à la connaissance de la commission spéciale ont principalement porté sur l'**absence de transposition de certaines dispositions figurant dans les directives** telles que des définitions de périmètre d'activité, d'incidents et de délais. Ces omissions ont pu être qualifiées de « sous-transposition législative » avec le risque d'une « sur-transposition réglementaire » dont ni les acteurs concernés, ni la commission n'ont obtenu de précisions satisfaisantes de la part du Gouvernement. Ainsi **le tableau synoptique des mesures d'application du projet de loi recense 40 renvois à la prise d'un décret en conseil d'État**.

3. LES APPORTS DE LA COMMISSION SPÉCIALE

La commission spéciale a adopté 61 amendements dont 53 de ses rapporteurs pour préciser les modalités de transposition des 3 directives. En outre, les rapporteurs ont décidé de réserver pour la discussion en séance publique le dépôt de plusieurs amendements nécessitant **des éclaircissements et des engagements du Gouvernement**.

A. PRÉCISER LES MODALITÉS DE TRANSPOSITION

18 amendements du rapporteur Hugues Saury, dont 6 amendements rédactionnels, complètent et encadrent les définitions et délais d'application (REC et NIS 2)

- **Transposer la définition des notions d'incident et de résilience** (article 1er), d'incident et de vulnérabilité (article 6) conformément à la lettre de la directive ;
- **Modifier la composition de la commission des sanctions** pour en renforcer les garanties d'indépendance (article 1er) ;

- **Étendre le champ de l'analyse des dépendances** devant être réalisée par les opérateurs d'importance vitale aux sous-traitants (article 1er) ;

- **Différer l'entrée en vigueur du titre Ier** pour éviter que certains opérateurs ne soient soumis à des délais raccourcis pour satisfaire à leurs obligations (article 4).

---

27 amendements du rapporteur Patrick Chaize, dont 10 amendements rédactionnels, visent à clarifier les obligations pesant sur les entités assujetties (NIS 2)

- **Inscrire dans la loi l'élaboration par le Gouvernement d'une stratégie nationale de cybersécurité** et les modalités de contrôle parlementaire de son application (article 5 *bis*) ;

- **Inscrire dans la loi la liste des secteurs hautement critiques** et critiques (article 7) et les modalités de sa mise à jour (article 12) ;

- **Élever la supervision de la cybersécurité au niveau des organes de direction** des entités et veiller à l'**exigence de proportionnalité des obligations** qui leur sont imposées (article 14) ;

- **Préciser les modalités de notification des incidents à l'ANSSI**, notamment en supprimant la notion d'« incident critique », qui, dans le projet de loi, vient s'ajouter à celui d'« incident important », ce qui est source de complexité inutile (article 17) ;

- **Encadrer le coût des contrôles restant à la charge des entités contrôlées** en le limitant aux seuls cas où des manquements sont constatés (article 29) ;

- **Préciser les règles de nomination des personnalités qualifiées** au sein de la commission de sanction (article 36).

---

8 amendements du rapporteur Michel Canévet, dont 2 amendements rédactionnels, visent trois objectifs (DORA)

- **Éviter des différences de traitement** injustifiées entre les entreprises par l'application du règlement DORA aux succursales d'entreprises d'investissement de pays tiers (article 49) ;

- **Simplifier la vie des entreprises**, en créant un guichet unique de notification des cyber-incidents (article 43 A), en fusionnant des dispositifs de déclarations d'incidents (article 49) et en évitant le double assujettissement à la directive NIS 2 et au paquet DORA (article 62 A) ;

- **Modérer les effets des surtranspositions** en supprimant l'article 53, qui introduisait une précision superfétatoire et sans doute contreproductive concernant les pouvoirs du secrétaire général de l'Autorité de contrôle prudentiel et de résolution, et en reportant l'entrée en vigueur du titre III de la loi au 1er janvier 2030 pour les sociétés de financement (article 62), auquel le règlement DORA ne fait pas référence.

En outre, **8 amendements déposés respectivement par Mmes Audrey Linkenheld (1), Catherine Morin-Desailly (2), Vanina Paoli-Gagin (1) et M. Mickaël Vallet (4)** ont apporté des précisions sur les notions d'activité d'importance vitale, sur la nature des risques à évaluer (article 1er), sur l'accompagnement par l'ANSSI des entités assujetties (article 5), sur la demande d'avis de la CNIL sur le décret définissant les informations à transmettre (article 12) et leur limitation au seul domaine cyber (article 23).

B. DES POINTS DE VIGILANCE QUI NÉCESSITENT DES ÉCLAIRCISSEMENTS ET DES ENGAGEMENTS DU GOUVERNEMENT

Dans la perspective de la séance publique, les rapporteurs envisagent de déposer des amendements qui nécessiteront des engagements de la part du Gouvernement :

- **Faire passer les communautés d'agglomération qui ne comptent aucune ville de 30 000 habitants** de la catégorie des entités essentielles vers la catégorie des entités importantes afin de ne pas leur faire supporter une charge disproportionnée ;

- **Trouver une définition législative d'une « labellisation NIS 2 »** pour permettre aux entreprises de valoriser, vis-à-vis de leurs banques, de leurs assurances ou bien encore de leurs clients, leurs efforts en matière de cybersécurité ;
- **Différer les dispositions en matière de contrôle et de sanctions** pendant au moins trois ans, voire davantage pour certaines entités ;
- **Instaurer un mécanisme de reconnaissance mutuelle entre États membres** pour que les entités puissent se prévaloir du respect de leurs obligations au sein d'un des pays de l'Union européenne.

Enfin, **la commission spéciale a formulé plusieurs recommandations** quant à l'application du nouveau dispositif de résilience et de cybersécurité :

► **Veiller à la proportionnalité des obligations des entités assujetties** ;

► **Fournir un effort de simplification des mesures d'application réglementaires**, en se gardant de toute surtransposition réglementaire ;

► **Accompagner les collectivités territoriales** dans cette démarche nouvelle pour elles en tenant compte des problématiques de compétences et de financement ;

► **Communiquer et faire œuvre de pédagogie, à l'échelle du pays**, sur l'effort de résilience et de cybersécurité, en lien avec la stratégie nationale de cybersécurité.

POUR EN SAVOIR +

- **Voir les travaux de la commission sépciale et les auditions publiques en vidéo (cliquer ici)**

Olivier Cadic
Président de la commission spéciale
Sénateur représentant les Français établis hors de France
(UC)

Page de la commission spéciale cybersécurité
https://www.senat.fr/travaux-parlementaires/structures-temporaires/commissions-speciales.html

Consulter le dossier législatif
https://www.senat.fr/dossier-legislatif/pjl24-033.html

Michel Canévet
Rapporteur
Sénateur du Finistère
(UC)

Patrick Chaize
Rapporteur
Sénateur de l'Ain
(LR)

Hugues Saury
Rapporteur
Sénateur du Loiret
(LR)