N° 393

SÉNAT

SESSION ORDINAIRE DE 2024-2025

Enregistré à la Présidence du Sénat le 4 mars 2025

RAPPORT

FAIT

au nom de la commission spéciale (1) sur le projet de loi relatif à la **résilience** *des* **infrastructures critiques** *et au* **renforcement** *de la* **cybersécurité** *(procédure accélérée),*

Par MM. Michel CANÉVET, Patrick CHAIZE et Hugues SAURY,

Sénateurs

(1) Cette commission est composée de : M. Olivier Cadic, *président ;* Mme Hélène Conway-Mouret, M. Bernard Fialaire, Mmes Michelle Gréaume, Nadège Havet, Christine Lavarde, Audrey Linkenheld, M. Akli Mellouli, Mme Vanina Paoli-Gagin, MM. Cédric Perrin, André Reichardt, *vice-présidents ;* MM. Étienne Blanc, Rémi Cardon, Mme Catherine Morin-Desailly, *secrétaires ;* Mmes Florence Blatrix Contat, Sophie Briante Guillemont, MM. Laurent Burgoa, Michel Canévet, Patrick Chaize, Mme Patricia Demas, MM. Thomas Dossus, Fabien Gay, Mme Sylvie Goy-Chavent, MM. Ludovic Haye, Loïc Hervé, Stéphane Le Rudulier, Mme Anne-Catherine Loisier, MM. Claude Malhuret, Damien Michallet, Mmes Laurence Muller-Bronn, Corinne Narassiguin, MM. Cyril Pellevat, Rémy Pointereau, Mme Olivia Richard, MM. David Ros, Hugues Saury, Mickaël Vallet.

Voir les numéros :

Sénat : **33** et **394** (2024-2025)

SOMMAIRE

Pages

L'ESSENTIEL

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

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 ;

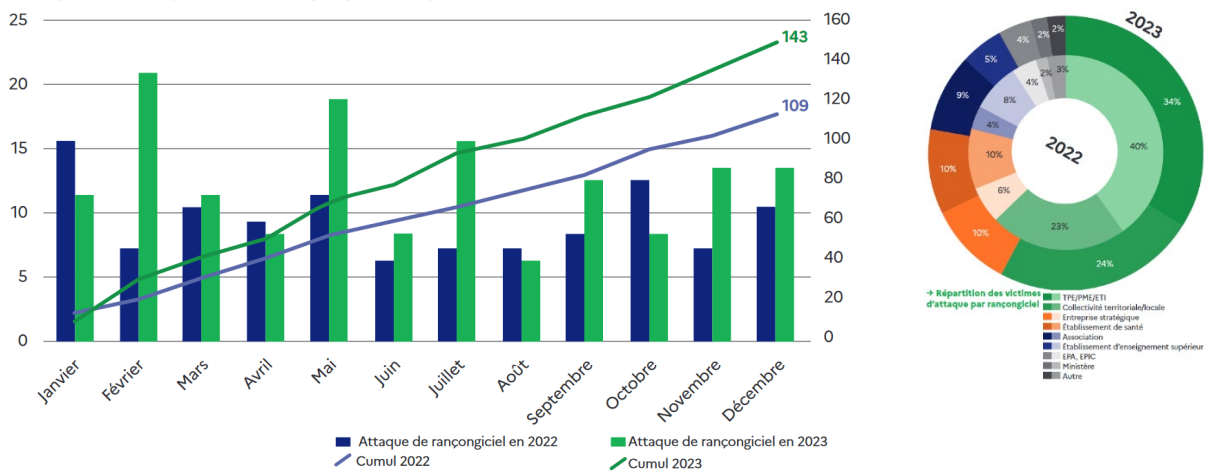
- la directive *Network and Information Security* (NIS 2), visant à assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union, va porter les 6 secteurs essentiels actuels à 18 secteur critiques et élargir le périmètre de régulation à 15 000 entités essentielles et importantes et près de 1 500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

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

***

La commission spéciale, présidée par Olivier Cadic, 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 Michel Canévet, Patrick Chaize et Hugues Saury.

La montée de la cybermenace illustrée par les attaques de rançongiciels



Source : ANSSI – Panorama de la cybermenace 2023

I. 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 ;

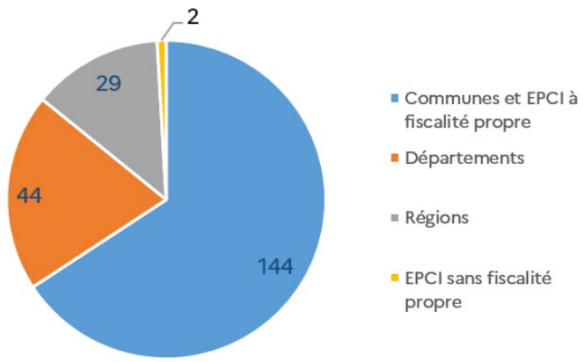
► Les attaques à caractère social, exploitant les vulnérabilités humaines.

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

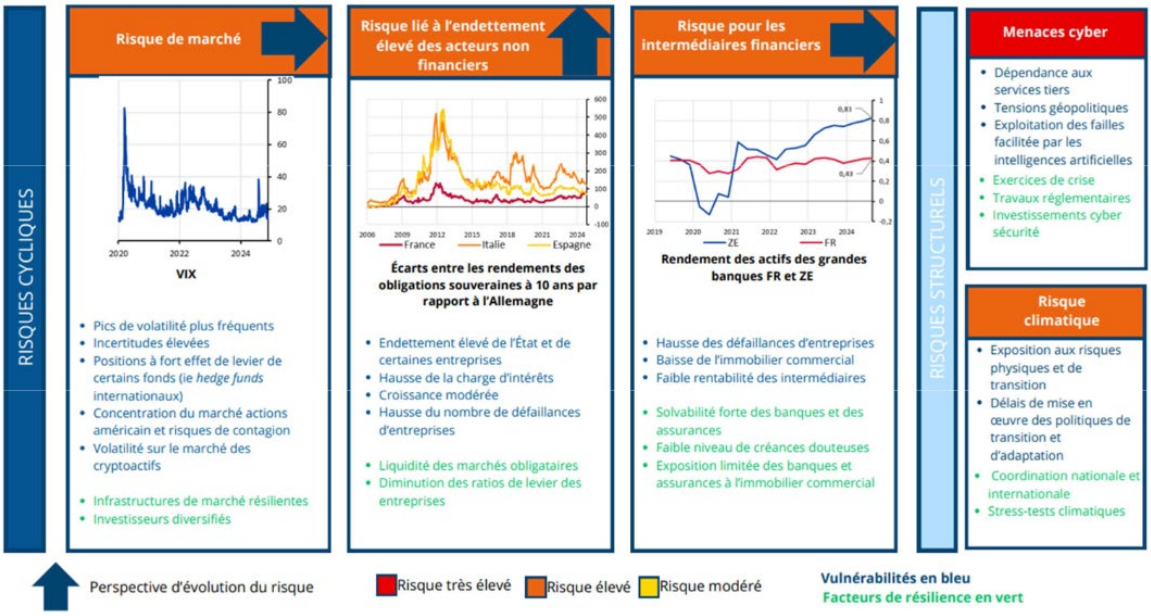
Le titre III du projet de loi transpose dans le droit interne les dispositions de la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 en ce qui concerne la résilience opérationnelle numérique du secteur financier, dite « DORA ».

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 cyber incident 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 (cf. graphique ci-après).

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**.

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

A. UNE TRANSPOSITION TARDIVE MAIS SUR LAQUELLE 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**.

Signe que ce texte mobilise le Sénat dans son ensemble, **la commission des affaires européennes**, présidée par Jean-François Rapin, a effectué une **communication sur les dispositions de transposition et d'adaptation** prévues par ce projet de loi[1], dont les observations ont été communiquées à l'ensemble des membres de la commission spéciale. L'observation principale concerne **l'assujettissement des sociétés de financement aux obligations de la directive DORA**, alors même que cela n'est pas prévu par la directive, cette surtransposition n'étant pas jugée préoccupante dans la mesure où ces entités peuvent constituer une porte d'entrée pour les cybermenaces. D'agissant des directives REC et NIS 2, la commission des affaires européenne ne constate « *aucune surtransposition notable* », tout en précisant que « *les latitudes laissées à*

[1] *Communication de la commission des affaires européennes sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (13 février 2025).*

chaque État membre pour la transposition ont néanmoins été utilisées de façon extensive par la France ».

III. 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. DES MODALITÉS DE TRANSPOSITION À PRÉCISER

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.

C. RECOMMANDATIONS SUR L'APPLICATION DU NOUVEAU DISPOSITIF

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.

EXAMEN DES ARTICLES

TITRE IER
RÉSILIENCE DES ACTIVITÉS D'IMPORTANCE VITALE

CHAPITRE IER
DISPOSITIONS GÉNÉRALES

Article 1er

Transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC)

Cet article vise à transposer en droit français la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, dite directive « REC ». ***Il renforce le dispositif actuel de sécurité des activités d'importance vitale (SAIV) instauré en 2006 en procédant à une actualisation du code de la défense****.*

La commission spéciale a adopté l'article premier modifié par 14 amendements des rapporteurs visant à :

- apporter des améliorations rédactionnelles et corriger une erreur matérielle ;

- définir les notions de « résilience » et d' « incident » ;

- clarifier la date à partir de laquelle une astreinte journalière pourra être appliquée ;

- inclure dans l'analyse des dépendances, qui devra être réalisée par les opérateurs d'importance vitale, l'analyse des vulnérabilités de leur chaîne de sous-traitance ;

- prévoir d'une part, que la notification d'incident doit intervenir au plus tard 24 heures après que l'opérateur en a pris connaissance, et d'autre part que le décret en Conseil d'État mentionné à l'alinéa 44 déterminera l'ensemble des conditions de mise en œuvre de cette obligation de notification ;

- étendre l'applicabilité du moyen de démontrer la conformité aux règles de sécurité, prévue à l'article 15 du présent projet de loi, aux opérateurs d'importance vitale qui ne sont ni soumis à la directive « NIS 2 » en tant qu'entité essentielle ou importante, ni soumis à la directive « REC » ;

- modifier la composition de la commission des sanctions afin d'en renforcer les garanties d'indépendance.

Elle a par ailleurs adopté 4 amendements tendant à préciser la notion d'activité d'importance vitale (COM-31), la nature des risques devant être évalués par les opérateurs d'importance vitale (COM-35), les critères de définition des entités critiques d'importance européenne particulière (COM-42) et les conditions de mise en œuvre d'une mission de conseil par la Commission européenne (COM-43).

La commission a adopté cet article ainsi modifié.

I. LE DROIT EXISTANT – DEPUIS 2006, LA FRANCE EST DOTÉE D'UN DISPOSITIF DESTINÉ À ASSURER LA SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

Mis en place en 2006, et inscrit dans le code de la défense aux articles L. 1332-1 à L. 1332-7 du code de la défense, **le dispositif de sécurité des activités d'importance vitale (SAIV) a pour objectif de protéger certains opérateurs, qu'ils soient publics ou privés, considérés comme essentiels pour garantir la continuité des activités ayant trait, de manière difficilement substituable ou remplaçable, à la production et la distribution de biens ou de services indispensables, ou qui, dans certains cas, pourraient représenter un danger significatif pour la population**.

Ces biens ou services doivent être indispensables :

- à la satisfaction des besoins essentiels pour la vie des populations ;
- ou à l'exercice de l'autorité de l'État ;
- ou au fonctionnement de l'économie ;
- ou au maintien du potentiel de défense ;
- ou à la sécurité de la Nation.

Un arrêté du Premier ministre du 2 juin 2006[1], modifié par un arrêté du 3 juillet 2008[2], fixe la liste des 12 secteurs d'activités d'importance vitale couverts par ce dispositif, qui concerne actuellement plus de **300 opérateurs d'importance vitale** (OIV). Ces derniers sont définis à l'article L. 1332-1 du même code comme « *les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* ». Les OIV exercent leurs activités sur **environ 1 500 points d'importance vitale** (PIV), dont la protection est garantie par le secret de la défense nationale. **Ils sont tenus, à leurs frais, d'assurer la sécurité de leurs sites et de leurs systèmes d'information les plus sensibles contre toute menace ou risque, notamment ceux à caractère terroriste**.

---

[1] *Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.*

[2] *Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.*

Les modalités de mise en œuvre du dispositif de SAIV sont fixées par l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale n°6600/SGDSN/PSE/PSN du 7 janvier 2014 (IGI 6600) de laquelle sont issus les développements qui suivent.

A. LES ACTEURS DE LA SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

1. Au niveau national

Le Premier ministre est chargé de la mise en place du cadre général du dispositif de SAIV en fixant la liste des secteurs, en désignant les ministres coordonnateurs desdits secteurs, en déterminant la méthode d'analyse et de gestion du risque ainsi que la méthode à suivre pour déterminer, par secteur d'activités d'importance vitale, les scénarios de menace et leur hiérarchisation selon le type ou le niveau de menace envisagé, et en élaborant les plans-type des plans de sécurité opérateur (PSO), des plans particuliers de protection (PPP) et des plans de protection externe (PPE) (cf. *infra*).

Il supervise la mise en place du dispositif et oriente la stratégie de sécurité des activités d'importance vitale.

Le SGDSN coordonne le dispositif de SAIV. Il assure la présidence et le secrétariat de la commission interministérielle de défense et de sécurité (CIDS). Il est l'entité de synthèse nationale en ce qui concerne la progression de la réalisation des PSO et des PPP.

La CIDS a un rôle consultatif. Son avis est notamment sollicité sur :

- la désignation des OIV, sur proposition des ministères coordonnateurs (cf. *infra*) ;

- les directives nationales de sécurité (DNS), à l'exception de celles relevant du ministre chargé la défense ;

- les PSO, à l'exception de ceux relevant du ministre chargé de la défense, dont le périmètre dépasse celui d'une zone de défense ;

- la liste des PIV annexée aux PSO, avec la possibilité de proposer des ajouts et des suppressions.

Chacun des 12 secteurs d'activité couverts par le dispositif de SAIV est en outre suivi par un ministère coordonnateur.

Secteur	Ministre coordonnateur
1 - Activités civiles de l'État (ACE)	Ministre de l'intérieur
2 - Activités judiciaires	Ministre de la justice
3 - Activités militaires de l'État (AME)	Ministre de la défense
4 - Alimentation	Ministre chargé de l'agriculture
5 - Communications électroniques, audiovisuel et information	Ministre chargé des communications électroniques
6 - Energie	Ministre chargé de l'énergie
7 - Espace et recherche	Ministre chargé de la recherche
8 - Finances	Ministre chargé de l'économie et des finances
9 - Gestion de l'eau	Ministre chargé de l'écologie
10 - Industrie	Ministre chargé de l'industrie
11 - Santé	Ministre chargé de la santé
12 - Transports	Ministre chargé des transports

Les ministres coordonnateurs veillent à l'application du dispositif de SAIV dans les secteurs d'activités dont ils ont la charge et au sein desquels ils :

- élaborent la ou les DNS correspondantes ;

- sélectionnent et prennent les décisions de désignation des OIV après avis de la CIDS ;

- instruisent les PSO de ses OIV ;

- transmettent les PSO à la CIDS ou à la CZDS suivant le cas de figure (à l'exception du ministre chargé de la défense) ;

- prennent les décisions de désignation des PIV.

En raison de la nécessité de protection du secret de la défense, le ministre chargé de la défense, ministre coordonnateur du secteur des activités militaires de l'État (AME), bénéficie de dispositions dérogatoires au schéma général de mise en œuvre du dispositif de SAIV.

Par ailleurs, outre son rôle de ministre coordonnateur du secteur d'activités « activités civiles de l'État », et sans préjudice des compétences nationales, générales et interministérielles dévolues au SGDSN et des compétences de coordination nationale des ministres dans le secteur d'activité

dont ils sont coordonnateurs, **l'animation de la mise en œuvre territoriale est assurée par le ministère de l'intérieur, *via* les services du haut fonctionnaire de défense (SHFD)**.

2. À l'échelle territoriale

Le préfet de zone de défense et de sécurité est chargé de la coordination du dispositif de SAIV. Il préside la commission zonale de défense et de sécurité (CZDS).

La CZDS est chargée d'une mission générale de coordination, d'assistance, et de contrôle de la mise en œuvre des PPP (à l'exception de ceux dépendant d'OIV relevant du ministre chargé de la défense). La commission, qui dispose d'un rôle consultatif, est sollicitée sur :

- les PSO des OIV dont le périmètre d'activité ne dépasse pas le ressort de la zone défense. Les PSO sont transmis à la CZDS par l'autorité administrative ayant désigné l'opérateur ;

- la liste des PIV annexée au PSO des OIV de son périmètre avec la capacité de proposer des ajouts ou suppressions ;

- la désignation et le périmètre exact d'une zone d'importance vitale ainsi que sur le PPP de zone d'importance vitale qui lui est transmis par le préfet de département ayant créé ladite zone ;

- la désignation, par un préfet de département, d'un OIV qui gère exclusivement un établissement mentionné à l'article L. 511-1 du code de l'environnement[1] ou comprenant une installation nucléaire de base, quand la destruction ou l'avarie de certaines installations de cet établissement peut présenter un danger grave pour la population, et la désignation du PIV correspondant.

Sur demande de son président ou du préfet de département concerné, la commission peut également donner un avis sur les plans de protection externe.

Enfin, le préfet de département est chargé de la mise en œuvre du dispositif de SAIV en application de la compétence générale qui lui est attribuée de conduite interministérielle des actions de l'État.

Cette responsabilité s'exerce notamment pour la protection externe des PIV, via le PPE. Il veille à la réalisation effective des mesures de sécurité

[1] *Les usines, ateliers, dépôts, chantiers et, d'une manière générale, les installations exploitées ou détenues par toute personne physique ou morale, publique ou privée, qui peuvent présenter des dangers ou des inconvénients soit pour la commodité du voisinage, soit pour la santé, la sécurité, la salubrité publiques, soit pour l'agriculture, soit pour la protection de la nature, de l'environnement et des paysages, soit pour l'utilisation économe des sols naturels, agricoles ou forestiers, soit pour l'utilisation rationnelle de l'énergie, soit pour la conservation des sites et des monuments ainsi que des éléments du patrimoine archéologique.*

prévues dans les PPP. Il peut saisir la CZDS de toute question qu'il juge utile. Sur convocation du préfet de zone, il participe à la CZDS.

Ses responsabilités particulières sont les suivantes :

- approbation du PPP des PIV des opérateurs ne relevant pas du ministre chargé de la défense, et du PPP des zones d'importance vitale ;

- décision d'équivalence entre un plan de protection réalisé au titre d'une autre réglementation, et le PPP ;

- élaboration du PPE de chaque PIV ou ZIV, en liaison avec le DDS de ce point ou de cette zone ;

- désignation des zones d'importance vitale (ZIV) après avis de l'officier général de la zone de défense et de sécurité lorsque celle-ci inclut un PIV relevant du ministère chargé de la défense ;

- désignation des OIV qui gèrent exclusivement un établissement mentionné à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base, quand la destruction ou l'avarie de certaines installations de cet établissement peut présenter un danger grave pour la population, et désignation du PIV correspondant ;

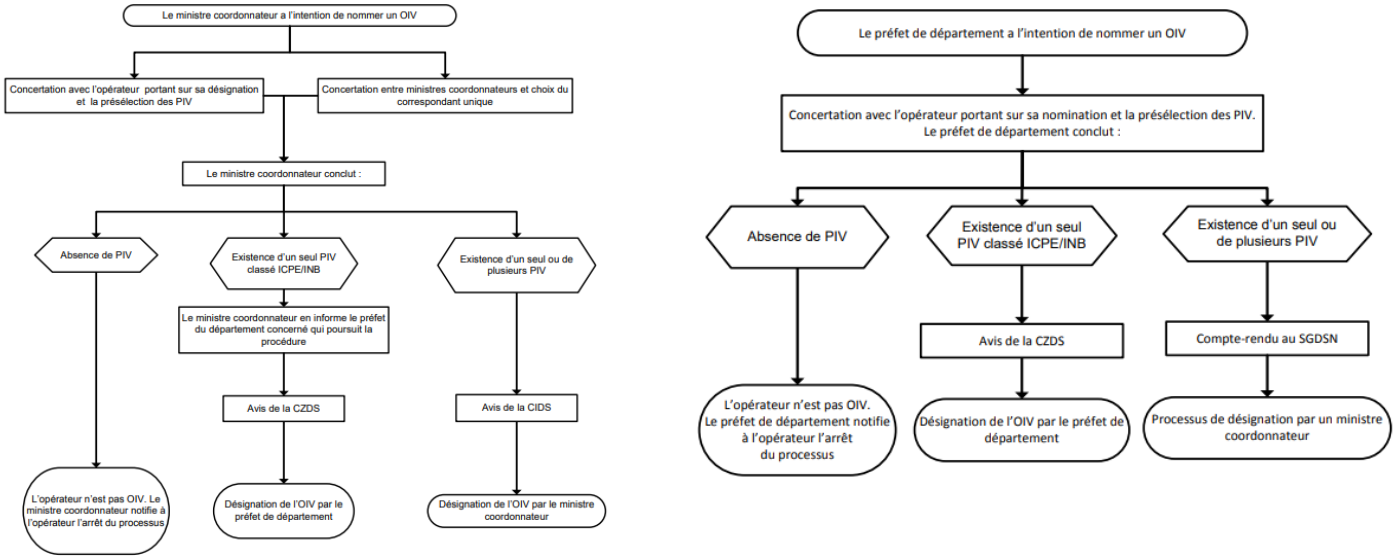
- mise en demeure de l'opérateur d'établir un PPP ;

- mise en demeure de l'opérateur d'exécuter une mesure de son PPP ;

- injonction à l'opérateur de modifier son PPP.

B. PROCESSUS DE DÉSIGNATION D'UN OIV ET D'UN PIV

Processus de désignation d'un opérateur d'importance vitale (OIV) initié par un ministre coordonnateur et par un préfet de département

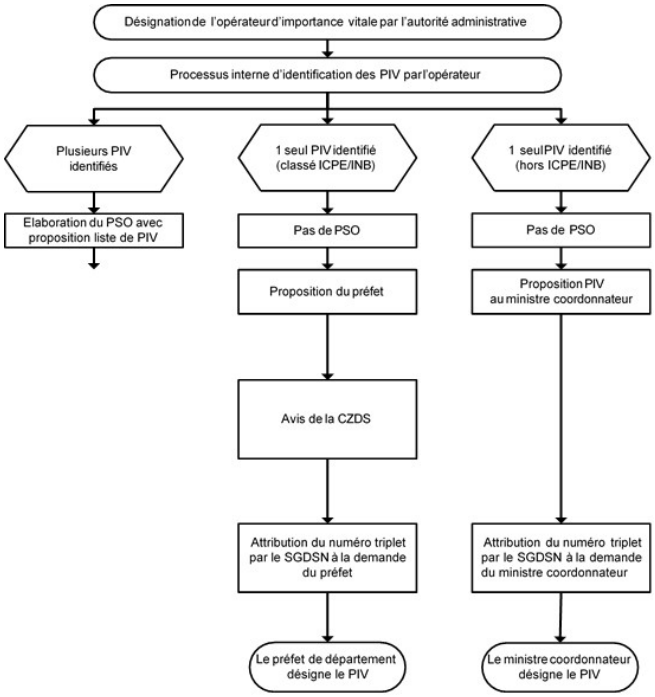


ICPE : installations classées pour la protection de l'environnement

INB : installations nucléaires de base

Source : étude d'impact

Processus de désignation d'un point d'importance vitale



C. LE PROCESSUS DE PLANIFICATION

Le processus de planification, c'est-à-dire d'élaboration des documents présentant les mesures de protection et de continuité d'activité des opérateurs, auquel les OIV doivent se soumettre, **découle d'une évaluation des risques et des menaces retracées au sein des directives nationales de sécurité (DNS)**.

La DNS s'applique à tout ou partie d'un secteur d'activités d'importance vitale. Elle décrit le périmètre du secteur ou du sous-secteur, elle en identifie les responsables, les processus et les enjeux et en définit le besoin de sécurité des fonctions essentielles. À la suite d'une analyse de risque dans laquelle sont énoncés et hiérarchisés les scénarios de menace, elle précise les objectifs et les politiques de sécurité du secteur ou du sous-secteur concerné. À cette fin, la DNS peut notamment définir la nature des opérateurs et des infrastructures susceptibles d'être désignés d'importance vitale au titre dudit secteur et préciser les critères de leur désignation.

Les DNS sont approuvées par arrêté du Premier ministre, après avis de la CIDS, puis transmises par le SGDSN aux ministres concernés, qui les relaient aux préfectures et aux services déconcentrés.

Sur la base des prescriptions de la ou des DNS qui leur ont été communiquées, les opérateurs sont tenus d'établir des documents de planification spécifiques (**plan de sécurité opérateur ou PSO et plan particulier de protection ou PPP**), qui comportent :

- l'identification des points d'importance vitale (PIV) ;

- l'analyse des risques et menaces susceptibles de les affecter (catastrophes naturelles, risques technologiques, pandémies, malveillance, cyberattaques, terrorisme, etc.) ;

- l'intégration des mesures Vigipirate propres à leur secteur d'activité ;

- l'établissement de **plans de continuité ou de reprise d'activité** (PCA/PRA) ;

- la désignation d'un délégué à la défense et à la sécurité (DDS), habilité au secret de la défense nationale et chargé de dialoguer avec le ministère coordonnateur. Un délégué local peut également être nommé pour chaque PIV ;

- la mise en œuvre de mesures garantissant la protection des informations classifiées, comme le statut d'OIV ou la liste des PIV.

Les documents de planification prévus dans le dispositif actuel de sécurité des activités d'importance vitale

Le plan de sécurité opérateur (PSO), prévu aux articles R. 1332-19 à R. 1332-22 du code de la défense, est destiné à définir la politique et l'organisation de la sécurité pour les opérateurs d'importance vitale (OIV). Il repose sur une analyse des risques et prend en compte les directives nationales de sécurité (DNS). Ce document précise les mesures organisationnelles, préventives et protectrices à mettre en œuvre pour chaque point d'importance vitale (PIV). Il est obligatoire uniquement si l'opérateur gère plusieurs PIV.

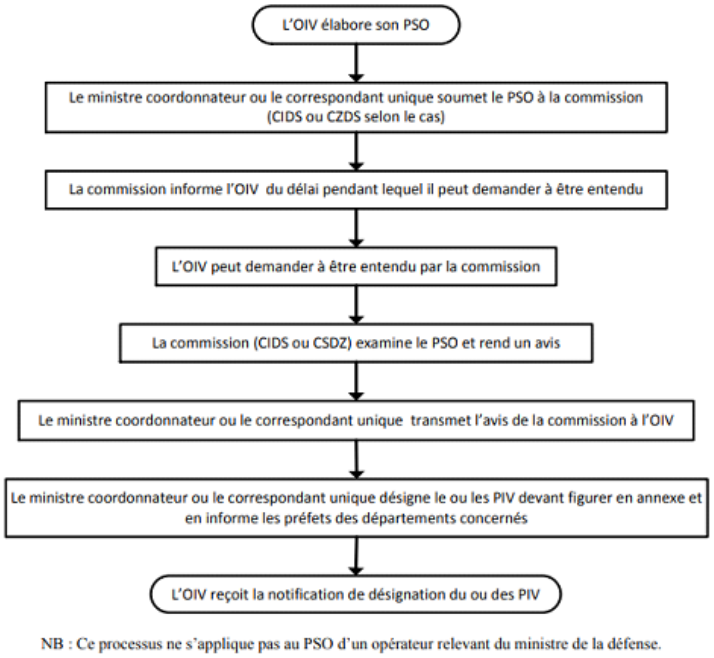
Le plan particulier de protection (PPP) de chaque point d'importance vitale est établi à partir du plan de sécurité d'opérateur d'importance vitale qui lui est annexé. Il comporte des mesures permanentes de protection et des mesures temporaires et graduées. Il prévoit aussi les délais de réalisation de ces mesures (article R. 1323-24 du code de la défense).

Le plan de protection externe (PPE) est un document classifié, élaboré par le préfet de département pour les PIV, en complément du PPP. Il précise les modalités d'intervention des forces de sécurité en cas d'agression sur le PIV, et décrit les moyens humains et matériels nécessaires. Sa rédaction implique les acteurs clés comme la gendarmerie ou la sécurité publique, et il doit être testé et actualisé régulièrement. Le PPE peut aussi inclure des mesures de contrôle des zones périphériques et organiser les échanges d'informations avec l'opérateur du PIV. Le PPE doit être communiqué aux services compétents, tout en préservant le secret de la défense nationale (article R. 1332-32 du code de la défense).

Aux termes du 3° de l'article R. 1332-18 du code de la défense, **les plans types des plans de sécurité d'opérateurs d'importance vitale, des plans particuliers de protection et des plans de protection externe sont fixés par arrêtés du Premier ministre, après avis de la CIDS**.

Enfin, **le plan de continuité d'activité** (PCA) a pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal (article L. 2151-4 du code de la défense).

Schéma du processus d'élaboration du plan de sécurité opérateur pour les opérateurs ne relevant pas du ministère chargé de la défense



Source : étude d'impact

II. LE DISPOSITIF PROPOSÉ – LA MODIFICATION DU DISPOSITIF DE SAIV AU SEIN DU CODE DE LA DÉFENSE

A. UNE RÉVISION DU DISPOSITIF NATIONAL RENDUE NÉCESSAIRE PAR LA DIRECTIVE (UE) 2022/2557 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 14 DÉCEMBRE 2022 SUR LA RÉSILIENCE DES ENTITÉS CRITIQUES (REC)

Le 8 décembre 2008, l'Union européenne a adopté une directive[1] visant à identifier et désigner les infrastructures critiques européennes et à évaluer les besoins en matière de protection renforcée. **Ce texte, qui se limitait aux secteurs des transports et de l'énergie**, a introduit la notion d'« infrastructures critiques » et en a proposé une définition harmonisée à l'échelle européenne. Ces infrastructures sont ainsi constituées par « *un point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions.* ».

[1] *Directive 2008/114/CE du 8 décembre 2008*

La directive rappelle que la protection des infrastructures critiques relève principalement des États membres, ainsi que des propriétaires ou exploitants de ces infrastructures. Elle les incite à identifier celles ayant une dimension européenne, à les notifier aux autres États membres, et à mettre en place des points de contact et des plans de sécurité spécifiques pour leur protection. La Commission européenne peut, pour sa part, soutenir ces efforts en partageant des bonnes pratiques ou en proposant des formations.

Une évaluation menée par la Commission européenne en 2019 a mis en lumière la nécessité d'une mise à jour du dispositif. Celle-ci s'imposait face à l'émergence de nouvelles menaces, telles que l'aggravation du dérèglement climatique, l'usage accru des drones ou encore le développement de l'intelligence artificielle. L'évaluation a également souligné le besoin de **passer d'une approche centrée sur des infrastructures isolées à une logique de protection des « entités »**, comprenant non seulement des infrastructures, mais aussi des réseaux (eau, énergie, communication) et des services essentiels.

Face à ces enjeux, l'Union européenne a adopté, le 14 décembre 2022, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (dite directive REC).

Négociée pour l'essentiel sous présidence française du Conseil de l'Union européenne (PFUE), cette directive établit un cadre minimal à l'échelle européenne afin d'assurer la « résilience » de tous les opérateurs d'entités critiques dans les États membres, élargissant ainsi le champ d'action au-delà des seules infrastructures critiques européennes.

Selon cette directive, les « entités critiques » incluent toute entité publique ou privée désignée par un État membre dans des secteurs stratégiques (articles 2 et 6). Elle s'inscrit dans un cadre législatif cohérent, en complément de la directive (UE) 2022/2555 sur la sécurité des réseaux face aux cyberattaques (SRI 2) et de la directive (UE) 2022/2556 relative à la résilience numérique dans le secteur financier (DORA).

Définitions issues de l'article 2 de la directive REC

1) « entité critique », une entité publique ou privée qui a été désignée par un État membre conformément à l'article 6 comme appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe ;

2) « résilience », la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir ;

3) « incident », un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit ;

4) « infrastructure critique », un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel ;

5) « service essentiel », un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement ;

6) « risque », le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise ;

7) « évaluation des risques », l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident ;

8) « norme », une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil ;

9) « spécification technique », une spécification technique au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012 ;

10) « entité de l'administration publique », une entité reconnue comme telle dans un État membre conformément au droit national, à l'exclusion de l'organisation judiciaire, des parlements et des banques centrales, qui satisfait aux critères suivants :

a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial ;

b) elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique ;

c) elle est financée majoritairement par les autorités de l'État ou d'autres organismes de droit public de niveau central, ou sa gestion est soumise à un contrôle de la part de ces autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé, pour plus de la moitié, de membres désignés par les autorités de l'État ou d'autres organismes de droit public de niveau central ;

d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux.

La directive (UE) 2022/2557 impose 3 principales obligations aux États membres : i) développer une stratégie nationale, ii) évaluer les risques auxquels les entités critiques sont exposées, et iii) identifier ces entités. Les États membres doivent également désigner des autorités compétentes pour garantir l'application de ces dispositions et établir un point de contact unique pour les échanges transfrontaliers concernant la résilience des entités critiques.

De leur côté, les entités critiques doivent évaluer leurs propres risques et mettre en œuvre des mesures techniques, de sécurité et organisationnelles adaptées pour garantir leur résilience. Ces mesures peuvent figurer dans un plan spécifique et doivent inclure des mécanismes de notification rapide des incidents aux autorités compétentes, ainsi que des vérifications des antécédents des employés occupant des fonctions sensibles ou ayant accès aux systèmes stratégiques.

Enfin, la directive reconnaît une **« importance européenne particulière » à toute entité critique désignée par un État membre et opérant des services similaires dans au moins 6 États membres**.

Si la directive constitue un socle commun minimal, elle laisse aux États membres la liberté d'adopter des mesures nationales plus strictes. Elle prévoit en outre des clauses de sauvegarde, permettant aux États de ne pas appliquer ses dispositions à certaines entités liées à la défense ou à la sécurité nationale.

Le règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil identifie 11 secteurs couverts par la directive REC : i) énergie, ii) transports, iii) bancaire, iv) infrastructures des marchés financiers, v) santé, vi) eau potable, vii) eaux résiduaires, viii) infrastructures numériques, ix) administration publique, x) espace, xi) production, transformation et distribution de denrées alimentaires, chaque secteur comprenant plusieurs sous-secteurs.

La transposition de la directive REC se traduira par conséquent **par un élargissement du champ d'application du dispositif national actuel à plusieurs sous-secteurs dont les réseaux de chaleur et de froid, l'hydrogène ou encore l'assainissement**.

B. ARTICLES L. 1332-1 ET L. 1332-2 MODIFIÉS – DÉFINITIONS

L'article 1er du présent projet de loi introduit **3 définitions principales** :

1) les activités d'importance vitale (alinéa 7) définies comme « *les activités indispensables au fonctionnement de l'économie ou de la société ainsi qu'à la défense ou à la sécurité de la Nation* » ;

2) les infrastructures critiques (alinéa 8) définies comme « *tout ou partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système nécessaire à l'exercice d'une activité d'importance vitale ou dont une perturbation pourrait mettre gravement en cause la santé de la population ou l'environnement* ». Deux catégories d'infrastructures critiques sont distinguées :

i) les points d'importance vitale (PIV) définis comme « *les installations les plus sensibles, notamment celles qui sont difficilement substituables* » (alinéa 10) ;

ii) les systèmes d'information d'importance vitale définis comme « *les systèmes d'information nécessaires à l'exercice d'une activité d'importance vitale ou à la gestion, l'utilisation ou la protection d'une ou plusieurs infrastructures critiques* » (alinéa 11) ;

3) les opérateurs d'importance vitale (OIV), définis aux alinéas 12 à 17 qui modifient l'article L. 1332-2 du code de la défense. Comme l'a indiqué le SGDSN en audition, **le critère déterminant pour identifier un OIV restera celui de la non-substituabilité**.

L'alinéa 14 précise que l'autorité administrative pourra mentionner, dans l'acte de désignation, l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur, l'opérateur devant à ce titre être regardé comme une entité critique au sens de la directive REC.

Il convient de relever que le champ des OIV retenu dans la transposition est plus large que celui des « entités critiques » au sens de la directive REC. En effet, **il inclut les opérateurs « régaliens »** relevant de la défense ou de la sécurité nationale, **lesquels sont pourtant explicitement exclus du champ de la directive REC**.

Les dispositions du titre Ier du présent projet de loi ont en outre vocation à s'appliquer à **certaines collectivités territoriales**, comme cela est déjà le cas dans le cadre du dispositif existant de SAIV.

Au total, si le nombre d'entités concernées ne peut pas être connu dans le détail, leur liste étant couverte par le secret de la défense nationale, le SGDSN a indiqué en audition que **l'entrée en vigueur du présent projet de loi devrait entraîner une augmentation limitée du nombre d'OIV et de PIV, estimée à quelques dizaines**.

Le SGDSN a indiqué au rapporteur Hugues Saury que si les modalités de désignation des OIV et l'architecture de planification font l'objet de dispositions réglementaires en cours de rédaction, elles ont globalement vocation à être conservées par rapport au dispositif actuel.

Ainsi, le processus de désignation devrait comporter les phases suivantes :

- dialogue entre le ministère coordonnateur et l'opérateur, identifié selon les éléments (éventuellement des seuils) prévus par la ou les directives nationales de sécurité concernées (DNS) ;

- désignation par le ministre après avis de la commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale (CIDS) ou par le préfet de département après avis de la commission zonale de défense et de sécurité des secteurs d'activités d'importance vitale pour les OIV à PIV unique classé ICPE ou INB ;

- arrêté de désignation de l'opérateur d'importance vitale ;

- notification, à l'opérateur de la ou des DNS applicables.

C. ARTICLES L. 1332-3 À L. 1332-5 MODIFIÉS – OBLIGATIONS DES OIV DESTINÉES À ACCROÎTRE LEUR RÉSILIENCE

1. Établissement d'un « plan de résilience opérateur »

Aux termes de l'article L. 1332-3 du code de la défense tel que modifié par le présent article premier, les OIV seront tenus d'évaluer les risques de toute nature, y compris ceux liés au terrorisme (alinéa 20). **Cette analyse devra être réalisée dans un délai de 9 mois après leur désignation et actualisée au moins tous les 4 ans** (alinéa 21).

Sur la base de cette analyse, les OIV devront élaborer des mesures de résilience adaptées pour assurer la continuité de leurs missions essentielles et protéger leurs infrastructures critiques (alinéa 22). **Ces mesures devront être détaillées dans un « plan de résilience opérateur » (PRO), lequel devra être établi dans un délai de 10 mois suivant la désignation de l'opérateur** (alinéa 23). Ce plan, qui fusionnera le plan de sécurité opérateur et l'essentiel du plan de continuité d'activité (cf. *supra*), sera soumis à l'approbation de l'autorité administrative compétente. La nature des mesures qui devront y être retranscrites sera précisée par décret en Conseil d'État (alinéa 29).

L'alinéa 24 du présent article prévoit que lorsque des documents existants répondent déjà partiellement ou totalement aux exigences, l'autorité administrative pourra les reconnaître comme équivalents au plan de résilience. Comme l'indique l'étude d'impact, cette disposition permettra notamment à l'OIV « *de se servir d'un plan de continuité d'activité existant pour*

l'intégrer à son PRO dans la partie devant porter sur les obligations de résilience, sur validation du principe par l'autorité administrative qui aurait vérifié que le plan en question répond aux exigences du dispositif SAIV ». Il convient de préciser que les PRO faisant l'objet de nouveaux plans-types établis à la suite de la mise à jour de l'instruction générale interministérielle relative la sécurité des activités d'importance vitale (IGI 6600) et des directives nationales de sécurité et même si ces derniers reprendront en grande partie les éléments contenus dans les plans-type des PSO actuels, seuls certains éléments de fond, toujours à jour, des parties des PSO existants pourront être repris dans les futurs PRO. **Les PSO en tant que tels, nécessairement lacunaires au regard des nouveaux plans-type, ne pourront donc pas être assimilés au PRO**.

L'alinéa 28 prévoit que les opérateurs désignés au titre du danger grave pour la population pourront connaître des aménagements dans les mesures applicables, afin que soient privilégiés les impératifs de sécurité sur la continuité d'activité.

En cas de manquement d'un opérateur à ses obligations, l'autorité administrative pourra lui adresser une mise en demeure pour élaborer, modifier ou mettre en œuvre le plan (alinéa 25). **Cette mise en demeure sera assortie d'un délai minimum d'un mois et pourra s'accompagner d'une astreinte financière pouvant atteindre 5 000 euros par jour de retard** (alinéa 26). L'astreinte pourra également être prononcée à l'expiration du délai imparti par la mise en demeure en cas de non-respect de celle-ci par l'OIV (alinéa 27).

Contrairement aux sanctions, le prononcé d'une astreinte pourra concerner l'État, ses établissements publics administratifs, les collectivités territoriales ainsi que leurs groupements et leurs établissements publics administratifs.

2. Réalisation d'une analyse des dépendances

L'alinéa 30 modifie l'article L. 1332-4 du code de la défense et impose aux OIV **d'analyser leurs dépendances** à l'égard de l'ensemble des acteurs essentiels à leurs activités vitales, qu'ils soient nationaux, européens ou internationaux, et ce, à chaque étape de leur chaîne de production ou d'activité. Cette évaluation inclut une analyse approfondie des vulnérabilités dans les chaînes d'approvisionnement et doit mener à des mesures concrètes (alinéa 31).

3. Établissement d'un « plan particulier de résilience » pour chaque point d'importance vitale

L'article L. 1332-5 du code de la défense tel que modifié par les alinéas 32 à 37 du présent article 1er fixe **l'obligation pour les OIV d'établir un « plan particulier de résilience » (PPR) pour chaque PIV**, qui se substitue au « plan

particulier de protection » (cf. *supra*). Comme le précise l'étude d'impact, celui-ci « *a également pour vocation d'intégrer les éléments auparavant indiqués dans le PPE en annexe, ainsi qu'une partie des éléments qui pouvaient apparaitre auparavant dans le plan de continuité d'activité que l'opérateur devait effectuer au titre de l'article L. 2151-4* ». Ce nouveau plan, qui doit détailler les mesures de protection et de résilience prises pour chaque PIV, constitue une **obligation supplémentaire par rapport aux prescriptions de la directive REC, cette dernière n'imposant l'établissement d'un plan qu'à l'échelle de l'opérateur**.

Comme pour les plans de résilience opérateur, il est prévu qu'un document existant, élaboré dans le cadre d'accords internationaux régulièrement ratifiés ou approuvés, de lois ou de règlements, et décrivant des mesures de protection jugées suffisantes pour un point d'importance vitale, peut être reconnu comme équivalent au PPR (alinéa 34).

En cas de refus de l'opérateur d'élaborer, de modifier ou de mettre en œuvre un PPR, l'autorité administrative peut le **mettre en demeure** de satisfaire à ses obligations dans un délai fixé, qui doit être d'au moins un mois (alinéa 35). **Cette mise en demeure pourra s'accompagner d'une astreinte financière pouvant atteindre 5 000 euros par jour de retard** (alinéa 35). L'astreinte pourra également être prononcée à l'expiration du délai imparti par la mise en demeure en cas de non-respect de celle-ci par l'OIV (alinéa 37). Contrairement aux sanctions, le prononcé d'une astreinte pourra concerner l'État, ses établissements publics administratifs, les collectivités territoriales ainsi que leurs groupements et leurs établissements publics administratifs

Comme dans le dispositif actuel de SAIV, la mise en œuvre de l'ensemble des obligations rappelées *supra* restera à la charge des OIV (alinéa 16).

D. ARTICLE L. 1332-6 MODIFIÉ – ENQUÊTES ADMINISTRATIVES DE SÉCURITÉ

Le contrôle de l'accès aux sites d'importance vitale, permettant aux OIV de solliciter l'avis de l'autorité administrative compétente, a été institué par la loi n° 2011-267 du 14 mars 2011 dite « LOPPSI 2 » (loi d'orientation et de programmation pour la performance de la sécurité intérieure). Ce dispositif, inscrit à l'article L. 1332-2-1 du code de la défense, prévoit que cet **avis est rendu à la suite d'une enquête administrative**, laquelle peut donner lieu à la consultation du casier judiciaire de l'intéressé et à des traitements automatisés de données à caractère personnel (article L. 1332-1 du code de la défense).

En pratique, le service national des enquêtes administratives de sécurité réalise annuellement 700 000 enquêtes, dont 70 000 au titre des points d'importance vitale. Par ailleurs, la direction du renseignement et de la

sécurité de la défense effectue environ 300 000 enquêtes par an pour les points d'importance vitale relevant du ministère de la défense.

Les alinéas 38 à 43 du présent article 1er modifient l'article L. 1332-6 du code de la défense afin d'encadrer les conditions dans lesquelles un OIV peut solliciter l'avis de l'autorité administrative. Deux hypothèses sont ainsi distinguées :

- avant d'accorder une autorisation d'accès physique ou à distance à des points ou systèmes d'information d'importance vitale (alinéa 38). Les cas dans lesquels les accès physiques ou à distance peuvent justifier une demande d'avis sont précisés dans le PRO (alinéa 41) ;

- avant le recrutement ou l'affectation à des postes nécessitant de tels accès ou impliquant des fonctions sensibles (alinéa 39), lesquelles sont définies comme celles « *indispensables à la réalisation d'une activité d'importance vitale ou dont l'occupation expose l'opérateur à des vulnérabilités* ». Elles sont identifiées dans le plan de résilience de l'OIV (alinéa 40).

En cas d'avis défavorable, qui ne peut être rendu que si l'enquête révèle un risque pour l'activité vitale ou la sécurité d'une infrastructure critique, l'opérateur privé[1] doit refuser l'autorisation.

E. ARTICLE L. 1332-7 NOUVEAU – OBLIGATION DE NOTIFICATION DES INCIDENTS

Le dispositif actuel ne contraint pas les OIV à signaler à l'autorité administrative les incidents physiques rencontrés.

En application des articles 14 et 15 de la directive REC, **l'alinéa 44 du présent article instaure une obligation pour les OIV de signaler à l'autorité administrative tout incident pouvant compromettre la continuité de leurs activités d'importance vitale, dans un délai défini par décret en Conseil d'État.**

L'alinéa 45 prévoit **la possibilité pour l'autorité administrative d'informer le public lorsqu'elle estime qu'il est dans l'intérêt général de le faire**.

F. ARTICLES L. 1332-8 ET L. 1332-9 NOUVEAUX – DISPOSITIONS APPLICABLES AUX ENTITÉS CRITIQUES D'IMPORTANCE EUROPÉENNE PARTICULIÈRE

Les alinéas 48 à 50 introduisent un article L. 1332-8 nouveau au sein du code de la défense **imposant aux OIV qui assurent des services essentiels ou similaires dans au moins 6 États membres d'en informer l'autorité**

[1] *La personne publique pourra pour sa part directement refuser l'autorisation demandée, ce qui constitue une mesure de police ne pouvant pas être déléguée à une personne privée.*

administrative. Cette obligation s'applique au plus tard au moment de la présentation pour approbation de leur « plan de résilience opérateur ». **Ces opérateurs sont alors désignés comme « entités critiques d'importance européenne particulière »**.

Certains opérateurs relevant de secteurs régaliens, comme la sécurité nationale, la défense, le nucléaire ou d'autres activités sensibles, peuvent toutefois être exemptés de tout ou partie des obligations résultant des articles L. 1332-8 et L. 1332-9 dans des conditions déterminées par décret en Conseil d'État.

L'article L. 1332-9 du code de la défense, créé par les alinéas 51 et 52 du présent article 1er, prévoit **la possibilité pour les entités critiques d'importance européenne particulière de faire l'objet de missions de conseil menées par la Commission européenne**. Ces missions, conditionnées à l'accord préalable de l'autorité administrative française, visent à évaluer la conformité de l'opérateur à ses obligations et à proposer des mesures pour renforcer sa résilience. À cette fin, l'opérateur concerné est tenu de garantir l'accès aux informations, systèmes et installations nécessaires, tout en respectant les secrets protégés par la loi.

G. ARTICLE L. 1332-10 NOUVEAU – DISPOSITIFS TECHNIQUES CONCOURANT À LA PROTECTION DES INSTALLATIONS D'IMPORTANCE VITALE

L'alinéa 54 du présent projet de loi reprend les dispositions figurant à l'heure actuelle à l'article L. 1332-6-1 A du code de la défense au sein d'un article L. 1332-10 nouveau.

Ces dispositions prévoient la possibilité pour les services de l'État concourant à la défense nationale, à la sûreté de l'État et à la sécurité intérieure **de procéder, au moyen de caméras installées sur des aéronefs, à la captation, à l'enregistrement et à la transmission d'images à des fins de protection des établissements, installations et ouvrages d'importance vitale**.

H. ARTICLE L. 1332-11 NOUVEAU – SYSTÈMES D'INFORMATION D'IMPORTANCE VITALE

Si les entités relevant du champ de la directive REC sont automatiquement assujetties aux dispositions de la directive NIS 2, le champ des OIV tel que retenu dans le dispositif français étant plus large que celui de la directive REC, **il était nécessaire de prévoir une disposition spécifique en droit national pour soumettre les opérateurs concernés aux obligations prévues par le titre II du présent projet de loi**.

L'alinéa 58 crée ainsi un article L. 1332-11 au sein du code de la défense qui prévoit que les opérateurs d'importance vitale mettent en œuvre

les obligations prévues aux articles 14 et 16 et au premier alinéa de l'article 17 du présent projet de loi.

I. ARTICLES L. 1332-12 ET L. 1332-13 NOUVEAUX – HABILITATIONS ET CONTRÔLES

Les articles L. 1332-12 à L. 1332-14 du code de la défense, introduits par les alinéas 64 à 73, **définissent les prérogatives des agents chargés de contrôler le respect des obligations des OIV**. **Ils précisent également les conditions d'accès aux informations et lieux nécessaires à leurs missions, ainsi que les sanctions applicables en cas d'entrave à leur action**.

L'article L. 1332-12 nouveau prévoit que les agents spécialement désignés et assermentés par l'État sont habilités à rechercher et constater les infractions et manquements aux obligations qui leur incombent, à l'exception de celles résultant de la transposition de la directive NIS 2 en matière de cybersécurité (alinéa 64).

Aux termes de l'article L. 1332-13, ces agents disposent de pouvoirs étendus pour l'exercice de leurs missions (alinéas 65 à 68). Ils peuvent notamment :

- accéder aux locaux des OIV, aux lieux à usage professionnel ou d'exécution d'une prestation de services ;

- obtenir tout document nécessaire à l'accomplissement de leur mission auprès des administrations publiques, des établissements et organismes placés sous le contrôle de l'État et des collectivités territoriales ainsi que dans les entreprises ou services concédés par l'État, les régions, les départements et les communes ;

- recueillir, sur place ou sur convocation, tout renseignement, toute justification ou tout document nécessaire aux contrôles et peuvent, à ce titre, exiger la communication de documents de toute nature propres à faciliter l'accomplissement de leur mission et les obtenir ou en prendre copie, par tout moyen et sur tout support, ou procéder à la saisie de ces documents quels qu'en soient les détenteurs ;

- procéder, sur convocation ou sur place, aux auditions de toute personne susceptible d'apporter des éléments utiles à leurs constatations. Ils en dressent procès-verbal.

Tenus au secret professionnel, celui-ci ne peut cependant pas leur être opposé, sauf dans les cas prévus par l'article 226-13 du code pénal (alinéa 69).

Aux termes de l'article L. 1332-14 nouveau, les opérateurs contrôlés sont tenus de coopérer avec l'autorité administrative. **Toute obstruction à l'exercice des fonctions des agents habilités peut entraîner une sanction prononcée par la commission des sanctions** (cf. *infra*) **pouvant s'élever à**

10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial hors taxes de l'exercice précédent, le montant le plus élevé étant retenu (alinéas 71 et 72).

Ces dispositions ne s'appliquent toutefois pas à l'État et à ses établissements publics administratifs (alinéa 73).

J. ARTICLE L. 1332-14 À L. 1332-19 NOUVEAUX – SANCTIONS ET MISE EN PLACE D'UNE COMMISSION DES SANCTIONS

Les alinéas 76 à 94 remplacent le régime de sanctions pénales de l'article L. 1332-7 du code de la défense par un dispositif de sanctions administratives. Ces dernières seront prononcées par **une commission des sanctions** en cas de non-respect des obligations prévues par l'article 1er (article L. 1332-15 nouveau).

Aux termes de l'article L. 1332-16 nouveau, **cette commission est composée d'un membre du Conseil d'État** désigné par le vice-président du Conseil d'État et qui assure la présidence de la commission, **d'un membre de la Cour de cassation** désigné par le premier président de la Cour de cassation, **d'un membre de la Cour des comptes** désigné par le premier président de la Cour des comptes, et **de 3 personnalités qualifiées nommées par le Premier ministre en raison de leurs compétences dans le domaine de la sécurité des activités d'importance vitale**

Elle statue de manière impartiale, sur la base des rapports de contrôle, après avoir entendu l'opérateur ou son représentant.

L'alinéa 88 du présent article introduit un article L. 1332-17 qui fixe **le plafond des amendes pouvant être prononcées à 10 millions d'euros ou 2 % du chiffre d'affaires annuel**. **Ces niveaux de sanction sont identiques à ceux prévus par l'article 34 de 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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2016/1148 (**NIS2**).

L'article L. 1332-18 nouveau prévoit en outre que **la commission peut ordonner la publication de la sanction, les frais étant à la charge de la personne sanctionnée.**

Les administrations de l'État et ses établissements publics administratifs de même que les collectivités territoriales, leurs groupements et leurs établissements publics administratifs sont exclus du champ des OIV pouvant être sanctionnés par des amendes administratives en cas de manquement aux obligations qui leur incombent.

K. ARTICLES L. 1332-20 À L. 1332-22 NOUVEAUX – MARCHÉS PUBLICS ET CONTRATS DE CONCESSIONS RELATIVES À LA SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

Les alinéas 97 à 103 visent à permettre **aux opérateurs d'importance vitale de recourir aux régimes dérogatoires inscrits dans le code de la commande publique, qui exonèrent notamment de l'obligation de publicité et de mise en concurrence, pour certains de leurs marchés (**dispositif prévu par le titre II du livre V de la deuxième partie du code de la commande publique) **et contrats de concessions** (dispositif prévu par le I du livre II de la troisième partie du code de la commande publique)**.**

Le recours à ces dérogations n'est possible que sous **deux conditions cumulatives :**

- d'une part, ces marchés ou concessions doivent concerner *« la conception, la qualification, la fabrication, la modification, la maintenance ou le retrait des structures, équipements, systèmes, matériels, composants ou logiciels nécessaires à la protection des infrastructures critiques de l'opérateur ou dont le détournement de l'usage porterait atteinte aux intérêts essentiels de l'État* » ;

- d'autre part, « *cette protection ou la prévention de ce détournement d'usage ne peuvent être garanties par d'autres moyens* ».

III. LA POSITION DE LA COMMISSION – UNE TRANSPOSITION NÉCESSAIRE QUI PERMETTRA DE REHAUSSER LE NIVEAU DE PROTECTION ET DE RÉSILIENCE DES INFRASTRUCTURES CRITIQUES

Plutôt que de créer un dispositif *ad hoc*, source de complexité pour les opérateurs déjà soumis au système actuel de SAIV, le présent projet de loi procède à une actualisation de ce dernier. **Il conserve sa terminologie, sans adopter celle issue de la directive du 14 décembre 2022**. Cette approche ne pose pas de difficulté, dès lors que le champ couvert par le projet de loi inclut celui de la directive et reprend toutes les obligations qu'elle prévoit, comme l'a souligné le Conseil d'État dans son avis du 6 juin 2024[1]. **Le choix du Gouvernement de s'appuyer sur le dispositif existant est opportun dès lors que celui-ci est connu et maîtrisé par les opérateurs concernés, dont le champ ne devrait de surcroît pas évoluer significativement**.

D'une manière générale, les services de l'État entendus en audition ont par ailleurs relevé que les obligations nouvelles incombant aux OIV se traduiront par une augmentation de leur charge de travail. En dépit d'un

[1] *« Le Conseil d'État estime que cela ne soulève toutefois pas de difficulté, dès lors que le champ personnel et matériel retenu par le projet de loi inclut bien celui de la directive et que toutes les obligations qu'elle prévoit sont reprises ».*

contexte budgétaire contraint, **la question de l'adaptation de leurs moyens, notamment humains, devra être prise en compte**.

Le rapporteur a par ailleurs veillé à ce que toute surtransposition soit évitée. À cet égard, il considère que **les dispositions qui ne figuraient pas dans la directive REC se justifient au regard de l'objectif de protection et de résilience des activités essentielles à la Nation**.

Ainsi, **s'agissant du champ d'application,** l'extension de l'essentiel des dispositions du présent article 1er aux opérateurs « régaliens » se justifie pour deux raisons. D'une part car **ces opérateurs sont déjà soumis au dispositif actuel de SAIV, que le présent projet de loi ne fait qu'actualiser et compléter**, et d'autre part, car **leur exclusion aurait conduit à les soumettre à des exigences moindres alors que leurs activités revêtent, par essence, un caractère stratégique**.

S'agissant des définitions figurant à l'article 1er, dans son avis précité, le Conseil d'État a regretté **l'absence de définition de la notion de « résilience »,** alors que son acception dans la directive diffère de l'usage courant en raison de la prise en compte, dans la définition donnée par la directive REC, des notions de prévention et de protection. Il peut en outre être relevé que le présent article 1er impose aux opérateurs d'importance vitale l'adoption de mesures de résilience (alinéa 22), intégrées dans le plan de résilience opérateur, ou encore de mesures de protection et de résilience inscrites dans les plans particuliers de résilience (alinéa 32). **À l'initiative des rapporteurs, la commission spéciale a ainsi adopté un amendement COM-83 visant à en introduire la définition au sein de l'article 1er afin d'en renforcer la clarté**.

De même, constatant que la notion d'« incident » est au cœur du titre Ier du projet de loi – dont l'objectif est de renforcer la protection et la résilience des infrastructures critiques face aux incidents –, **la commission spéciale, sur proposition des rapporteurs, a adopté un amendement COM-82 visant à en préciser la définition.**

S'agissant des obligations qui incomberont aux OIV, d'une manière générale, les évolutions inscrites dans le présent article, qui consacrent le passage d'une logique de protection à une logique de résilience, vont dans le bon sens.

Contrairement à la directive, qui s'en tient aux plans élaborés à l'échelle des opérateurs eux-mêmes (plans de résilience), il est prévu que le dispositif national conserve les plans détaillés pour chaque point d'importance vitale. Ce modèle à deux niveaux, garantit un niveau d'exigence élevé pour les opérateurs les plus sensibles.

Par deux amendements COM-87 et COM-89 portés par les rapporteurs, le mécanisme d'astreinte journalière prévu aux alinéas 26 et 36 a été précisé. Il est désormais explicitement indiqué que cette astreinte pourra s'appliquer dès l'expiration du délai fixé dans la mise en demeure adressée par l'autorité administrative**.**

Le rapporteur Hugues Saury constate que l'article 12 de la directive REC ne prévoit pas la réalisation d'une analyse des dépendances par les entités critiques. Il considère cependant que cette mesure participe pleinement de l'objectif poursuivi tant par la directive que par le présent projet de loi.

Le contenu de cette analyse pourrait cependant être complété. La rédaction actuelle, limitée aux « chaînes d'approvisionnement » pourrait laisser entendre qu'elle ne concerne que les matières premières. Or les OIV peuvent également être très fortement dépendants de leurs sous-traitants. C'est pourquoi, **à l'initiative des rapporteurs, la commission spéciale a adopté un amendement COM-88 visant à étendre à l'analyse des dépendances devant être réalisée par les OIV à la chaîne de sous-traitance**.

S'agissant de l'obligation de notification des incidents prévue à l'article L. 1332-7 du code de la défense (nouveau), **la commission a adopté un amendement COM-90 rectifié des rapporteurs prévoyant, d'une part, que la notification d'incident doit intervenir au plus tard 24 heures après que l'opérateur en a pris connaissance, et d'autre part que le décret en Conseil d'État mentionné à l'alinéa 44 déterminera l'ensemble des conditions de mise en œuvre de cette obligation de notification**. Ce décret pourra notamment établir des exceptions liées à la protection du secret de la défense nationale et préciser la nature des incidents devant être signalés à l'autorité administrative.

Par ailleurs, sur proposition des rapporteurs, la commission a adopté un amendement COM- 92 visant à étendre l'applicabilité du moyen de démontrer la conformité aux règles de sécurité, prévue à l'article 15 du présent projet de loi, aux opérateurs d'importance vitale qui ne sont ni soumis à la directive « NIS 2 » en tant qu'entité essentielle ou importante, ni soumis à la directive « REC ».

Enfin, **le régime de sanctions prévu par l'article 1er reposant sur des sanctions administratives, apparaît plus opérant que les sanctions pénales actuelles qui n'ont jamais été appliquées**.

Il offre en outre de meilleures garanties aux opérateurs justiciables, avec la création d'une commission des sanctions. Afin d'en renforcer les garanties d'indépendance, **la commission spéciale a adopté un amendement COM-94 des rapporteurs prévoyant que les 3 personnalités qualifiées siégeant au sein de cette commission ne seront pas exclusivement nommées par le Premier ministre mais respectivement par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat**.

Par ailleurs, si **les plafonds de sanctions fixés par le présent article apparaissent élevés au regard de ceux qui ont pu être retenus dans d'autres États membres ayant déjà transposé la directive REC**, ceux-ci se justifient pour deux raisons. D'une part, **il est nécessaire que ces plafonds de sanctions aient un effet dissuasif**. D'autre part, **ces niveaux de sanctions sont alignés sur ceux prévus par la directive NIS 2, avec laquelle la directive REC doit**

former un ensemble cohérent. Il semble en outre pertinent que les sanctions liées aux mesures de protection et de résilience des infrastructures physiques ne soient pas moins élevées que celles appliquées au domaine cyber. En effet, la cybersécurité n'est qu'une sous-composante des risques globaux ; un déséquilibre en faveur de cette dernière pourrait entraîner un effet d'éviction de la résilience globale au profit exclusif de la cybersécurité.

Aussi, considérant que l'application de sanctions constitue en toute hypothèse un *ultima ratio*, le dispositif de SAIV reposant sur la coopération, il n'apparaît pas nécessaire de modifier les plafonds de sanction prévu par le présent article 1er.

La commission spéciale a par ailleurs adopté 6 amendements rédactionnels, de clarification, de précision ou visant à corriger une erreur matérielle des rapporteurs[1] et 4 amendements tendant à préciser :

- la notion d'activité d'importance vitale (amendement COM-31 de notre collègue Mickaël Vallet et les membres du groupe Socialiste, Écologiste et Républicain) ;

- la nature des risques devant être évalués par les opérateurs d'importance vitale (amendement COM-35 de notre collègue Mickaël Vallet et les membres du groupe Socialiste, Écologiste et Républicain) ;

- les critères de définition des entités critiques d'importance européenne particulière (amendement COM-42 de notre collègue Mickaël Vallet et les membres du groupe Socialiste, Écologiste et Républicain) ;

- les conditions de mise en œuvre d'une mission de conseil par la Commission européenne (amendement COM-43 de notre collègue Mickaël Vallet et les membres du groupe Socialiste, Écologiste et Républicain).

Décision de la commission : la commission spéciale a adopté l'article ainsi modifié.

[1] *COM-81, 84, 85, 86, 91 et 93.*

CHAPITRE II
DISPOSITIONS DIVERSES

Article 2

Actualisation de références législatives

Cet article procède à diverses actualisations de références au sein du code de la défense, du code pénal, du code des postes et des communications électroniques, du code de la santé publique, du code de la sécurité intérieure et de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information rendues nécessaires par les modifications introduites au sein du code de la défense par l'article 1er du présent projet de loi.

La commission spéciale a adopté cet article sans modification.

I. LE DISPOSITIF PROPOSÉ - UNE ACTUALISATION DE RÉFÉRENCES LÉGISLATIVES TIRANT LES CONSÉQUENCES DES MODIFICATIONS APPORTÉES PAR L'ARTICLE 1ER DU PRÉSENT PROJET DE LOI

Le présent article vise à actualiser au sein du code de la défense, du code pénal, du code des postes et des communications électroniques, du code de la santé publique, du code de la sécurité intérieure et de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information afin de prendre en compte les modifications introduites au sein du code de la défense par l'article 1er du présent projet de loi.

Ainsi, les références :

- aux seuls opérateurs visés actuellement à l'article L. 1332-1 du code de la défense[1] sont modifiées pour renvoyer aux opérateurs d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 tel que modifié par l'article 1er du présent projet de loi [2] (modification des articles L. 1333-1 du code de la défense, 226-3 du code pénal, L. 33-14 et L. 34-11 du code des postes et des communications électroniques, et L. 1333-9 du code de la santé publique) ;

[1] *Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation*

[2] *Les opérateurs publics ou privés exerçant, au moyen d'infrastructures critiques situées sur le territoire national, une activité d'importance vitale*

- aux opérateurs visés aux articles L. 1332-1 et L. 1332-2[1] sont modifiées pour renvoyer à l'ensemble des opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 tel que modifié par le présent projet de loi (modification des articles L. 2113-2, L. 2151-1, L. 2171-6, L. 2321-2-1, L. 2321-3, L. 4231-6 du code de la défense, L. 33-1 du code des postes et communications électroniques, L. 223-2 et L. 223-8 du code de la sécurité intérieure et à l'article 15 de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information).

Par ailleurs, l'obligation d'élaborer des plans de continuité ou de rétablissement d'activité figurant à l'article L. 2151-4 du code de la défense est supprimée, ces documents devant être remplacés par le plan de résilience opérateur mentionné à l'article L. 1332-3 tel que modifié par l'article 1er du présent projet de loi.

II. LA POSITION DE LA COMMISSION

Le présent article, qui se borne à procéder à des actualisations de références législatives, n'appelle pas d'observations particulières de la commission spéciale.

Décision de la commission : la commission spéciale a adopté l'article sans modification.

[1] *Établissements mentionnés à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base visée à l'article L. 593-1 du code de l'environnement quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population*

Article 3

Dispositions relatives à l'outre-mer

Le présent article fixe les modalités d'application des dispositions de l'article 1er en outre-mer.

La commission a adopté cet article sans modification.

I. LE DISPOSITIF PROPOSÉ - FIXATION DES MODALITÉS D'APPLICATION DES DISPOSITIONS DE L'ARTICLE 1ER EN OUTRE-MER

Conformément à l'article L. 1 du code de la défense[1], les dispositions inscrites à l'article 1er du présent projet de loi au sein de ce même code sont applicables de plein droit sur l'ensemble du territoire de la République. Les modifications introduites par le présent projet de loi dans le code de la défense s'appliqueront par conséquent automatiquement aux collectivités relevant du principe de l'identité législative, à savoir la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon, ainsi qu'à celles soumises au principe de la spécialité législative, incluant les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises (TAAF).

Néanmoins, en tant que pays et territoires d'outre-mer (PTOM), Saint-Barthélemy, Saint-Pierre-et-Miquelon, Wallis-et-Futuna, la Polynésie française, la Nouvelle-Calédonie et les TAAF ne relèvent pas du droit de l'Union européenne. C'est pourquoi **les règles concernant les opérateurs d'importance vitale (OIV) fournissant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront pas applicables dans ces territoires, sauf adaptation spécifique**.

Les alinéas 2 et 3 créent un article L. 6221-2 au sein du code de la défense établissant un principe de substitution automatique des références à des dispositions inapplicables à Saint-Barthélemy par des références à des dispositions équivalentes applicables localement. Une telle disposition existe déjà à l'article L. 6311-1 pour Wallis-et-Futuna, la Polynésie française, la Nouvelle-Calédonie et les TAAF.

Par ailleurs, il est prévu que **les dispositions concernant les entités critiques d'importance européenne particulière ne sont pas applicables à**

[1] *Le code de la défense est applicable de plein droit sur l'ensemble du territoire de la République, à moins qu'il n'en dispose autrement.*

Saint-Barthélemy (article L. 6222-1 créé par les alinéas 4 et 5), **à Saint-Pierre-et-Miquelon** (article L. 6242-2 créé par les alinéas 6 et 7), **à Wallis-et-Futuna, en Polynésie française, en Nouvelle-Calédonie ni dans les TAAF** (article L. 6312-3 créé par les alinéas 8 et 9).

Le présent article modifie en outre plusieurs dispositions relatives à l'outre-mer au sein du code pénal, du code des postes et des communications électroniques et du code de la sécurité intérieure afin de faire référence à la présente loi :

- 711-1 du code pénal (alinéa 10) ;
- L. 33-1, L ; 33-15 et L. 34-14 du code des postes et des communications électroniques (alinéas 11 à 14) ;
- L. 285-1, L ; 286-1, L. 287-1 et L 288-1 du code de la sécurité intérieure (alinéa 15).

II. LA POSITION DE LA COMMISSION

Les dispositions proposées n'appellent pas de commentaire de la part de la commission, qui se déclare favorable à son adoption.

Décision de la commission : la commission spéciale a adopté l'article sans modification.

CHAPITRE III
DISPOSITIONS TRANSITOIRES

Article 4

Dispositions transitoires

Cet article fixe les obligations applicables aux opérateurs d'importance vitale désignés avant l'entrée en vigueur du titre Ier de la présente loi.

La commission a adopté l'article 4 modifié par un amendement COM-95 des rapporteurs visant à différer l'entrée en vigueur du titre Ier.

I. LE DISPOSITIF PROPOSÉ - UNE ADAPTATION DES DÉLAIS DE MISE EN ŒUVRE POUR LES OPÉRATEURS D'IMPORTANCE VITALE DÉSIGNÉS AVANT L'ENTRÉE EN VIGUEUR DU TITRE IER

Le présent article vise à adapter les délais de mise en œuvre des obligations inscrites à l'article 1er du présent projet de loi pour les opérateurs d'importance vitale (OIV) désignés avant l'entrée en vigueur du titre Ier.

En premier lieu, l'alinéa 1er du présent article prévoit que **les OIV actuels seront considérés comme désignés à partir de l'entrée en vigueur du présent titre Ier**, c'est-à-dire, en l'absence de disposition spécifique inscrite dans le présent projet de loi, au lendemain de la publication de la présente loi au Journal officiel. À ce titre, ils seront soumis aux obligations suivantes :

- réalisation d'une analyse des risques de toute nature et d'un plan de résilience opérateur (article L. 1332-3 modifié du code de la défense) ;

- analyse de leurs dépendances à l'égard des tiers (article L. 1332-4 modifié du code de la défense) ;

- réalisation d'un plan particulier de résilience (article L. 1332-5 modifié du code de la défense) ;

- respect des obligations résultant du titre II du présent projet de loi relatif à la cybersécurité.

Or **trois délais courent à partir de la désignation en tant qu'OIV** :

- 9 mois pour la réalisation d'une analyse des risques de toute nature ;

- 9 mois pour la réalisation d'une analyse des dépendances à l'égard des tiers ;

- 10 mois pour la réalisation du plan de résilience opérateur.

L'alinéa 2 du présent article dispose quant à lui que **ces opérateurs demeureront soumis à leurs obligations antérieures jusqu'à l'accomplissement des obligations inscrites à l'article 1er du présent projet de loi**, afin d'éviter tout « vide » juridique les concernant.

II. LA POSITION DE LA COMMISSION - DES DISPOSITIONS TRANSITOIRES NÉCESSAIRES MAIS QUI DOIVENT ÊTRE PRÉCISÉES

Si la mise en place de dispositions transitoires pour les OIV désignés avant l'entrée en vigueur du présent projet de loi est nécessaire, la rédaction actuelle de l'article 4 pourrait leur être défavorable, ainsi qu'aux OIV désignés après cette entrée en vigueur mais avant la publication de l'ensemble des actes d'application (décrets, directives nationales de sécurité, plans-types, etc.).

En effet, si le deuxième alinéa de cet article prévoie que les OIV désignés avant l'entrée en vigueur du présent titre Ier puissent continuer à se conformer à leurs obligations actuelles, aux termes de l'alinéa 1er, **les délais fixés aux deuxième[1] et quatrième alinéas de l'article L. 1332-3[2] ainsi qu'à l'article L. 1332-4[3] du code de la défense, dans leur version modifiée par le présent projet de loi, commenceront néanmoins à courir dès cette entrée en vigueur**.

Or, la publication des actes d'application pourrait prendre plusieurs mois, réduisant d'autant le temps laissé aux opérateurs pour se conformer à leurs nouvelles obligations. Il n'est d'ailleurs pas exclu que ces actes soient adoptés après l'expiration des délais prévus, rendant impossible le respect des délais légaux. **Cette situation concernerait également les OIV désignés après l'entrée en vigueur de la loi mais avant la publication de l'ensemble des actes d'application**.

C'est pourquoi, **sur proposition des rapporteurs, la commission spéciale a adopté un amendement COM-95 prévoyant de différer l'entrée en vigueur du titre Ier à une date fixée par décret en Conseil d'État, et au plus tard un an après la promulgation de la présente loi**.

Les OIV désignés avant cette date demeureront soumis aux obligations du dispositif de sécurité des activités d'importance vitale en vigueur jusqu'à l'expiration des délais fixés aux deuxième et quatrième alinéas de l'article L. 1332-3 ainsi qu'à l'article L. 1332-4 du code de la défense.

---

1 Réalisation d'une analyse des risques de toute nature dans un délai de 9 mois à compter de la désignation en tant qu'OIV.

2 Élaboration d'un plan de résilience opérateur dans un délai de 10 mois à compter de la désignation en tant qu'OIV.

3 Réalisation d'une analyse des dépendances à l'égard de tiers dans un délai de 9 mois à compter de la désignation en tant qu'OIV.

Décision de la commission : la commission spéciale a adopté l'article ainsi modifié.

TITRE II
CYBERSÉCURITÉ

CHAPITRE IER
DE L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Article 5

Missions et compétences de l'autorité nationale

Cet article vise à consacrer l'Agence nationale de sécurité des systèmes d'information (ANSSI) comme cheffe de file, à l'échelon national, en matière de cybersécurité en plus de sa compétence antérieure dans le domaine de la cyberdéfense.

La commission spéciale a adopté un amendement COM-96 de précision des rapporteurs.

Elle a par ailleurs adopté un amendement COM-58 visant à étendre les missions de l'autorité nationale de sécurité des systèmes d'information à l'accompagnement et au soutien au développement de la filière cybersécurité.

La commission a adopté cet article ainsi modifié.

I. LE DROIT EXISTANT – À L'HEURE ACTUELLE, SEULE LA COMPÉTENCE EN MATIÈRE DE CYBERDÉFENSE EST EXPLICITEMENT RECONNUE À L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

L'article L. 2321-1 du code de la défense dispose que « *le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information.* ***Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de défense des systèmes d'information*** ».

L'article R. 2321-1 du code de la défense précise que « ***l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 est l'Agence nationale de sécurité des systèmes d'information*** » (ANSSI).

Il convient de préciser que **le ministre chargé de la défense dispose de compétences spécifiques en matière de sécurité des systèmes d'information d'importance vitale relevant du contrôle gouvernemental de**

la dissuasion nucléaire (articles R. 1411-11-36 à R. 1411-11-44 du code de la défense).

L'article 8 de 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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2016/1148 **(NIS 2) prévoit que «** ***chaque État membre désigne ou établit une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de supervision*** *[…]* ».

Or, en l'état actuel du droit, l'article L. 2321-1 du code de la défense précité attribue clairement à l'autorité nationale de sécurité des systèmes d'information la fonction de défense des systèmes d'information, mais pas celle de leur sécurité, seul l'article 3 du décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » disposant que « *l'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale en matière de sécurité des systèmes d'information* ».

Comme le relève l'étude d'impact du présent article, **les missions de l'autorité nationale en la matière ne font l'objet, au niveau législatif, que de mentions isolées au sein des codes des postes et des communications électroniques et du code monétaire et financier** (articles L. 33-1, L. 33-14 et L. 102 du code des postes et des communications électroniques, L. 631-1 du code monétaire et financier).

Cyberdéfense et cybersécurité

Les notions de cybersécurité et de cyberdéfense présentent ce lien d'interdépendance sans qu'elles recouvrent des périmètres identiques. Ainsi, la **cyberdéfense est l'«** ***ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité*** **»** tandis que **la cybersécurité est définie comme un «** ***état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace*** **»**.

La cyberdéfense met notamment en œuvre la lutte informatique défensive, définie comme un « *ensemble coordonné d'actions menées par un État, qui consistent à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant* » et **la lutte informatique offensive** définie comme un « *ensemble coordonné d'actions menées dans le cyberespace par un État contre des systèmes d'information ou de données pour les perturber, les modifier, les dégrader ou les détruire* ». Ce sont ces deux types d'actions de lutte qui figurent au titre des missions de l'autorité nationale de défense des systèmes d'information prévues à l'article L. 2321-1 et suivants du code de la défense.

Source : étude d'impact

II. LE DISPOSITIF PROPOSÉ - UNE CLARIFICATION DES COMPÉTENCES DE L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION EN MATIÈRE DE CYBERSÉCURITÉ

La transposition de la directive NIS 2 et notamment de son article 8 précité **nécessite que soit clairement désignée au moins une autorité chargée de la sécurité des systèmes d'information ainsi que du contrôle et de la supervision qui en découlent**.

Le présent article 5 dispose ainsi que « *l'autorité nationale de sécurité des systèmes d'information* ***est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle*** ».

Comme rappelé *supra*, l'article R. 2321-1 du code de la défense précisant que « *l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 est l'Agence nationale de la sécurité des systèmes d'information* », **le présent article 5 confie par conséquent cette mission à l'ANSSI**.

Il consacre ainsi l'Agence comme cheffe de file, à l'échelon national, de l'action gouvernementale et des différents services en matière de cybersécurité.

Conformément aux recommandations du Conseil d'État dans son avis du 6 juin 2024, le **présent article prévoit en outre la possibilité pour le Premier ministre de désigner un autre organisme que l'ANSSI pour exercer certaines de ses responsabilités à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense**.

L'alinéa 3 du présent article 5 renvoie à un décret en Conseil d'État le soin de préciser les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice.

Selon l'ANSSI, seront ainsi fixées au niveau réglementaire les missions de :

- centre national et gouvernemental de réponse aux incidents de sécurité numérique (prévue par les articles 10 et 11 de la directive NIS 2) ;

- certification, qualification, agrément, autorisation et labellisation, prévues par le cadre législatif national autant que par des règlementations européennes ;

- sécurisation des systèmes d'information de l'État et de certains opérateurs publics et privés, notamment au titre des dispositions du code de

la défense applicables aux activités d'importance vitale, et de celles issues de la directive NIS 2 ;

- sensibilisation et formation pour favoriser la prise en compte de la sécurité des systèmes d'information ;

- autorité de gestion de crise d'origine cyber (prévue à l'article 9 de la directive NIS 2).

Selon l'étude d'impact, le renvoi à un décret permettra en outre « *de préciser en quelles matières spécifiques certains ministères exerceront, dans le domaine de la défense, les compétences de l'autorité nationale de sécurité des systèmes d'information au sens de l'article 8 de la directive, préservant ce faisant la répartition des compétences existant actuellement* ».

III. LA POSITION DE LA COMMISSION - L'ANSSI, NÉCESSAIRE « CHEF D'ORCHESTRE » DE LA CYBERSÉCURITÉ AU NIVEAU NATIONAL

L'article 8 de la directive NIS 2 précité n'impose pas la désignation d'une autorité unique chargée de la cybersécurité et des tâches de supervision, à l'exception du domaine de la défense.

Le Gouvernement a cependant fait le choix de confier à une autorité unique, l'ANSSI, ces missions. Le rapporteur Hugues Saury considère que **l'ANSSI est un acteur qui a fait ses preuves depuis sa création en 2009 et qui est désormais clairement identifié par les différents acteurs**.

Dès lors, identifier un « chef d'orchestre » responsable de la coordination, à l'échelon national, de l'action gouvernementale et des différents services en matière de cybersécurité apparaît de bon sens et il ne semble pas opportun de remettre en cause ce choix.

Plusieurs personnes entendues en audition ont par ailleurs regretté le fait que les missions de l'autorité nationale de sécurité des systèmes d'information ne soient pas mentionnées dès le présent projet de loi. **Il convient néanmoins de relever qu'à l'heure actuelle les missions de l'ANSSI ne figurent pas dans la partie législative du code de la défense mais sont notamment inscrites à l'article 3 du décret du 7 juillet 2009 précité**.

En effet, s'agissant d'un service à compétence nationale, l'existence comme les missions de l'ANSSI ont vocation à être déterminées par un décret, conformément à l'article 2 du décret n°97-464 du 9 mai 1997 relatif à la création et à l'organisation des services à compétence nationale. En outre, de telles dispositions, qui ont trait à l'organisation de l'administration ressortent naturellement du domaine réglementaire.

À titre d'exemple, plusieurs services à compétence nationale voient leurs missions définies par voie réglementaire. Dans le périmètre du Secrétariat général de la défense et de la sécurité nationale (SGDSN), on peut

citer Viginum (créé par le décret n° 2021-922 du 13 juillet 2021), chargé de la vigilance et de la protection contre les ingérences numériques étrangères, ainsi que l'OSIIC (décret n° 2020-455 du 21 avril 2020), opérateur des systèmes d'information interministériels classifiés. En dehors du périmètre du SGDSN, l'Office national anti-fraude (ONAF, décret n° 2024-235 du 18 mars 2024) et la Trésorerie générale des douanes (décret n° 2024-223 du 14 mars 2024) constituent également des services à compétence nationale dont l'existence et les missions sont fixées par décret.

La commission spéciale a adopté un amendement COM-96 de précision des rapporteurs.

Elle a par ailleurs adopté un amendement COM-58 de notre collègue Catherine Morin-Desailly visant à étendre les missions de l'autorité nationale de sécurité des systèmes d'information à l'accompagnement et au soutien au développement de la filière cybersécurité.

Décision de la commission : la commission spéciale a adopté l'article ainsi modifié.

Article 5 bis (nouveau)

Stratégie nationale de cybersécurité

Cet article, introduit en commission par un amendement COM-97 des rapporteurs, prévoit que le Premier ministre élabore une stratégie nationale de cybersécurité qui devra être actualisée au moins tous les cinq ans.

I. LE DROIT EXISTANT

Aux termes de l'article 7 de 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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, « ***chaque État membre adopte une stratégie nationale en matière de cybersécurité*** *qui détermine les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs ainsi que les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir* ».

Si cet exercice est actuellement mené sous l'autorité du secrétaire général de la défense et de la sécurité nationale (SGDSN)[1], à l'occasion notamment de la rédaction des revues nationales stratégiques (RNS), **aucune disposition législative n'en fixe le cadre**.

II. LE DISPOSITIF PROPOSÉ

Cet article additionnel résulte de l'adoption par la commission de l'amendement COM-97 des rapporteurs.

Il transpose l'article premier de la directive (UE) 2022/25/55, lequel stipule « *la présente directive fixe des obligations qui imposent aux États membres d'adopter des stratégies nationales en matière de cybersécurité* » en prévoyant que le Premier ministre élabore une stratégie nationale de cybersécurité et en définisse le contenu.

Actualisée au moins tous les cinq ans, cette stratégie devra comprendre des indicateurs clés de performance aux fins de l'évaluation de sa mise en œuvre.

[1] *L'ANSSI a publié en 2011 une Stratégie nationale de défense et de sécurité des systèmes d'information, suivie d'une Stratégie nationale pour la sécurité du numérique présentée en 2015 par le Premier ministre, puis, en 2018, d'une Revue stratégique de cyberdéfense élaborée par le SGDSN.*

En outre, à partir de 2026, et tous les deux ans, le Gouvernement soumettra au Parlement, avant le 30 septembre, un rapport sur l'application de la stratégie nationale de cybersécurité.

Décision de la commission : la commission spéciale a adopté l'article additionnel.

CHAPITRE II
DE LA CYBER RÉSILIENCE
Section 1
Définitions

Article 6

Définitions

Cet article vise à définir les principales notions nécessaires pour la mise en œuvre du dispositif national de cybersécurité tel qu'imposé par la directive NIS 2.

La commission a adopté l'article 6 modifié par 2 amendements des rapporteurs tendant à définir les notions d'« incident » (COM-98) et de « vulnérabilité (COM-99)».

I. LE DISPOSITIF PROPOSÉ - UNE CLARIFICATION DU GLOSSAIRE NATIONAL EN MATIÈRE DE CYBERSÉCURITÉ

Le présent article définit 7 notions liées à la sécurité et à la résilience numériques, dont la définition est nécessaire pour l'application du dispositif national prévu par le titre II (bureau d'enregistrement, office d'enregistrement, prestataire de services de confiance, prestataire de services de confiance qualifié, représentant, service de centre de données et système d'information).

Plutôt que de reprendre l'ensemble des 41 définitions figurant à l'article 6 de la directive NIS 2[1], le présent article 6 se limite à celles :

- qui nécessitent une adaptation dans le droit national (bureau d'enregistrement[2] et office d'enregistrement[3]) ;

[1] *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, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).*

[2] *La directive parle d'*« entité fournissant des services d'enregistrement de noms de domaine ».

[3] *La directive parle de* « registre de noms de domaine de premier niveau ».

- qui permettent de préciser le cadre national (services de centre de données, prestataires de services de confiance qualifiés[1] et systèmes d'information).

II. LA POSITION DE LA COMMISSION - UN EFFORT DE DÉFINITION BIENVENU MAIS INCOMPLET

L'effort de définition porté par le présent article vise à lever toute ambiguïté s'agissant de notions nécessaires pour la mise en œuvre du dispositif normatif. Il s'inscrit ainsi dans l'objectif à valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi qui impose d'adopter des dispositions suffisamment précises et des formules non équivoques, comme l'a rappelé le Conseil constitutionnel dans sa décision n° 2005-514 DC du 28 avril 2005.

De nombreuses personnes entendues en audition ont cependant indiqué regretter **l'absence de définition de la notion d'incident**

Devant la commission spéciale[2], Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI), a précisé : « *il était évident que la notion d'incident, qui figurait dans la directive NIS 2, serait précisée par un acte d'exécution - il a été pris cet été.* ***Nous avons donc fait le choix de ne pas l'inscrire dans la loi, et de garder plutôt le levier réglementaire****. Nous procéderons éventuellement à quelques ajustements mineurs pour l'intégrer dans le cadre plus général des dispositions préexistantes, notamment en ce qui concerne les prestataires de services qualifiés, qui seront soumis à la même définition d'incident. Nous apporterons peut-être aussi des précisions pour en affiner l'interprétation.* ***Reste que nous avons bien l'intention de reprendre cette définition et de l'intégrer*** ».

De fait, si le règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 identifie 2 catégories principales d'incidents (incidents importants et incidents récurrent), il distingue 10 types d'incidents importants : i) incidents importants concernant les fournisseurs de services DNS, ii) incidents importants concernant les registres de noms de domaine de premier niveau, iii) incidents importants concernant les fournisseurs de services d'informatique en nuage, iv) incidents importants concernant les fournisseurs de services de centres de données, v) incidents importants concernant les fournisseurs de réseaux de diffusion de contenu, vi)

[1] *Les définitions des notions de prestataires de services de confiance et de prestataires de services de confiance qualifiés procèdent par renvois au règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE dit* « règlement eIDAS ». *Comme le relève l'étude d'impact :* « conformément à la directive NIS 2, qui vise uniquement les prestataires de services de confiance au sens du règlement eIDAS, seules les définitions prévues par la directive ont été reprises ».

[2] *Audition du 17 décembre 2024.*

incidents importants concernant les fournisseurs de services gérés et les fournisseurs de services de sécurité gérés, vii) incidents importants concernant les fournisseurs de places de marché en ligne, viii) incidents importants concernant les fournisseurs de moteurs de recherche en ligne, ix) incidents importants concernant les fournisseurs de plateformes de services de réseaux sociaux, et x) incidents importants concernant les fournisseurs de services de confiance.

Si reprendre l'ensemble de ces définitions au niveau législatif ne serait pas opportun, **une définition générale de la notion d'incident aurait pu être apportée dès le stade de la loi,** alors que celle-ci est centrale pour la mise en œuvre de plusieurs dispositions du présent projet de loi notamment les articles 14 concernant la mise en œuvre des mesures de résilience cyber, 17 sur l'obligation de notification des incidents significatifs, et 29 portant sur les contrôles de l'ANSSI.

Ainsi, sur proposition des rapporteurs, la commission spéciale a adopté un amendement COM-98 visant à intégrer la définition de l'incident telle que figurant dans la directive NIS 2 : « *un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles* ».

Cette définition pourra être précisée par voie réglementaire, notamment pour tenir compte des compléments apportés par le règlement d'exécution 2024/2690 du 17 octobre 2024.

Par ailleurs, **la notion de « vulnérabilité », qui figure à l'article 17 du présent projet de loi (obligation de notification), n'est pas plus définie**.

De même, **le présent projet de loi ne mentionne à aucun moment l'importance du facteur humain, alors que celui-ci est à l'origine de nombreuses attaques**.

C'est pourquoi, sur proposition des rapporteurs, la commission spéciale a adopté un amendement COM-99 visant à reprendre la définition de la notion de vulnérabilité figurant à l'article 6 de la directive NIS 2 précité en faisant figurer une mention relative aux vulnérabilités d'origine humaine.

Décision de la commission : la commission spéciale a adopté l'article ainsi modifié.

Article 7

Liste des secteurs d'activité « hautement critiques » et « critiques » du point de vue de la cybersécurité

Cet article renvoie à un décret en Conseil d'État l'établissement de la liste des secteurs d'activité considérés comme « hautement critiques » et « critiques » du point de vue de la cybersécurité, alors que cette liste est pourtant établie clairement par les annexes I et II de la directive NIS 2.

La commission a adopté l'article 7 modifié par un amendement tendant à inscrire dans la loi la liste des secteurs d'activité considérés comme « hautement critiques » et « critiques » du point de vue de la cybersécurité en reprenant la liste établie par les annexes I et II de la directive NIS 2.

I. La situation actuelle – la directive NIS 1 avait identifié six secteurs essentiels en matière de cybersécurité, auxquels la France avait rajouté de sa propre initiative huit secteurs supplémentaires, la directive NIS 2 prévoyant pour sa part dix-huit secteurs « hautement critiques » ou « critiques »

1) La situation résultant de la directive NIS 1 : l'identification de six secteurs essentiels, auxquels la loi française de transposition avait ajouté huit secteurs supplémentaires

La directive NIS 1 avait identifié **six secteurs « essentiels »** auxquels s'appliquaient les dispositions qu'elle prévoyait **en matière de cybersécurité**.

Ces secteurs, jugés **prioritaires** en raison de **leurs effets potentiellement systémiques**, étaient les suivants :

- l'énergie ;
- les transports ;
- les banques ;
- les infrastructures de marchés financiers ;
- la santé ;
- la fourniture et la distribution d'eau potable ;
- les infrastructures numériques.

La loi n° 2018-133 du 26 février 2018[1] transposant la directive NIS 1 avait **rajouté**, au niveau français, **huit secteurs** à la liste établie par la directive.

Il s'agissait des secteurs suivants :

- les assurances ;
- la restauration collective ;
- le traitement des eaux ;
- les organismes sociaux ;
- l'emploi et la formation professionnelle ;
- l'éducation.

Sur la base de ces dispositions et du choix de ces secteurs, **263 opérateurs de services essentiels (OSE)** ont été désignés en France depuis 2016.

Les OSE sont **des opérateurs tributaires des réseaux ou systèmes d'information**, qui fournissent **un service essentiel** dont **l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société**.

Avec ce premier dispositif, ces grands acteurs ont été soumis à **l'obligation de déclarer leurs incidents de sécurité à l'Anssi**, et de **mettre en œuvre les mesures de sécurité nécessaires** pour **réduire fortement l'exposition de leurs systèmes les plus critiques aux risques cyber**.

Les OSE étaient désignés selon un processus, relativement **lourd administrativement**, impliquant **la consultation des ministères** sur l'identité des opérateurs à désigner, la transmission d'un courrier d'intention de désignation à chaque opérateur, une réponse officielle à la prise en compte des remarques faites par l'Anssi puis **la désignation individuelle par arrêté du Premier ministre**.

Le décret n° 2018-384 du 23 mai 2018 fixait notamment **les règles de sécurité que les entités régulées devaient respecter**, dont l'élaboration et la mise en œuvre **d'une politique de sécurité des réseaux et systèmes d'information** ou **la détection et le traitement des incidents de sécurité affectant les réseaux et systèmes d'information**.

2) La situation nouvelle créée par NIS 2, qui prévoit une liste de dix-huit secteurs « hautement critiques » ou « critiques »

Le texte de la directive NIS 1 prévoyait que la Commission européenne réexamine périodiquement **le fonctionnement global du dispositif** et **évalue la liste des secteurs et sous-secteurs** dans lesquels **sont identifiés des opérateurs de services essentiels (OSE)** et les types de services numériques couverts par la directive.

---

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*

Comme rappelé *supra*, dès 2018 la France avait **prévu d'intégrer des secteurs d'activité qui n'étaient pas couverts par la directive NIS 1**. **La directive NIS 2** est allée plus loin **en intégrant de nouveaux secteurs d'activité**.

Cette liste des dix-huit secteurs « hautement critiques » et « critiques » est établie respectivement par **les annexes I et II de la directive NIS 2**.

Celle-ci prévoit ainsi, à son annexe I, que **constituent des secteurs « hautement critiques »** les secteurs suivants, les secteurs en gras constituant des secteurs nouveaux :

- l'énergie, dont électricité, réseaux de chaleur et de froid, pétrole, gaz et hydrogène ;
- les transports, dont transport aériens, transports ferroviaires, transports par eau et transports routiers ;
- les banques ;
- les infrastructures des marchés financiers ;
- la santé ;
- l'eau potable ;
- **les eaux usées ;**
- l'infrastructure numérique ;

la gestion des services TIC (interentreprises) ;

- **l'administration publique (dont les activités ne portent pas sur la sécurité nationale, sécurité publique, la défense ou l'application de la loi) ;**
- **l'espace**.

Constituent pour leur part **des secteurs « critiques »** au sens de l'annexe II de la directive NIS 2 les secteurs suivants :

- **les services postaux et d'expédition** ;
- **la gestion des déchets** ;
- **la fabrication, la production et la distribution de produits chimiques** ;
- **la production, transformation et distribution des denrées alimentaires** ;
- **la fabrication, dont la fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro ; la fabrication de produits informatiques, électroniques et optiques, la fabrication d'équipements électriques ; la fabrication de machines et équipements n.c.a ; la construction de véhicules automobiles,**

remorques et semi-remorques ; la fabrication d'autres matériels de transport ;

- **les fournisseurs numériques** ;
- **la recherche**.

II. Le dispositif envisagé – une transposition qui renvoie à un décret en Conseil d'État l'établissement de la liste des secteurs « hautement critiques » et « critiques » en droit interne

Dans le but de **transposer les deux annexes de la directive NIS 2**, l'article 7 du présent projet de loi dispose que **la liste des secteurs d'activité « hautement critiques » et « critiques »** pour le fonctionnement de l'économie et de la société mentionnés dans la section 2 « Des exigences de sécurité des systèmes d'information » du projet de loi **est fixée par décret en Conseil d'État**.

Il est donc proposé de **renvoyer au niveau réglementaire la transposition précise des deux annexes de la directive établissant la liste des secteurs « hautement critiques » et « critiques » d'un point de vue de la cybersécurité** auxquels s'appliquent les exigences de sécurité des systèmes d'information prévues par la présente loi. **Or il s'agit d'un point essentiel pour définir le champ d'application de ces dispositions**.

III. La position de la commission – l'inscription dans la loi de la liste des secteurs « hautement critiques » et « critiques » du point de vue de la sécurité des systèmes d'information

La commission spéciale considère qu'il n'est **pas acceptable que des dispositions aussi importantes que la liste** des secteurs « hautement critiques » et « critiques » d'un point de vue de la cybersécurité auxquels s'appliquent les exigences de sécurité des systèmes d'information prévues par la présente loi **soient renvoyées à un décret en Conseil d'État**.

Il s'agit là **d'un élément clef, incontournable pour déterminer si une entité est ou non régulée par les dispositions de transposition de la directive NIS 2**.

C'est la raison pour laquelle la commission spéciale a adopté **un amendement COM 100 du rapporteur Patrick Chaize reprenant exactement les dispositions des annexes I et II de la directive NIS 2** pour prévoir que sont considérés au titre de la section 2 « Des exigences sécurité des systèmes d'information » comme **des secteurs « hautement critiques » pour le fonctionnement de l'économie et de la société** les secteurs :

- de l'énergie ;
- des transports ;
- des banques ;

- des infrastructures des marchés financiers ;

- de la santé ;

- de l'eau potable ;

- des eaux usées ;

- de l'infrastructure numérique ;

- de la gestion des services des technologies de l'information et de la communication ;

- de l'espace.

Cet amendement prévoit également que sont considérés au titre de la section 2 « Des exigences sécurité des systèmes d'information » comme **des secteurs « critiques » pour le fonctionnement de l'économie et de la société** les secteurs :

- des services postaux et d'expédition ;

- de la gestion des déchets ;

- de la fabrication, de la production et de la distribution de produits chimiques ;

- de la production, de la transformation et de la distribution des denrées alimentaires ;

- de la fabrication de certains biens, équipements et produits ;

- des fournisseurs numériques ;

- de la recherche.

Afin de laisser au Gouvernement **les marges de manœuvre nécessaires**, l'amendement prévoit qu'un décret en Conseil d'État **précise les modalités d'application de l'article 7** et détermine les sous-secteurs et les types d'entités relevant des secteurs « hautement critiques » et « critiques ».

Cela devrait notamment permettre de **tenir compte de l'évolution parfois fluctuante des périmètres ministériels**, sujet sur lequel l'Anssi avait indiqué à vos rapporteurs qu'il fallait conserver **une certaine souplesse pour permettre une bonne exécution du titre II du présent projet de loi**.

La commission a adopté cet article ainsi modifié.

Article 8

Définition des entités « essentielles » du point de vue de la sécurité des systèmes d'information

Cet article vise à préciser la liste des entités considérées comme « essentielles » du point de vue de la sécurité des systèmes d'information et qui, à ce titre, se verront appliquer les dispositions prévues par le présent projet de loi en transposition de la directive NIS 2.

La commission a adopté cet article sans modification.

I. La situation actuelle – face à une menace cyber croissante, la directive NIS 2 fait le choix d'imposer un rehaussement du niveau de cybersécurité des systèmes d'information de nombreuses entités

1) Un risque cyber devenu systémique et qui ne se limite plus aux grandes entreprises ou aux infrastructures critiques

Comme la ministre chargée du numérique et le directeur de l'Anssi l'ont rappelé lors de leurs auditions devant la commission spéciale, **la menace cyber a largement changé de nature au cours des dix dernières années**.

Alors qu'elle ciblait avant tout **les grandes entreprises** ou **les infrastructures critiques**, souvent à des fins **d'espionnage stratégique et industriel** ou **de déstabilisation**, et était souvent **d'origine étatique**, elle est devenue **systémique** et émane de plus en plus **de groupes cybercriminels organisés**, qui opèrent avant tout **dans un but lucratif**, et utilisent **des outils d'attaque** parfois **accessibles** à **des acteurs aux compétences techniques limitées**.

L'exploitation de vulnérabilités « jour-zéro »[1] et « jour-un »[2], liée à **des retards dans l'application des correctifs** par les entités visées, est par exemple **particulièrement utilisée par ces groupes criminels**.

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

- les attaques par raçongiciel, 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 ;

[1] *Il s'agit d'une vulnérabilité n'ayant fait l'objet d'aucune publication ni correctif de sécurité au moment de son exploitation.*

[2] *Il s'agit d'une vulnérabilité pour laquelle un correctif de sécurité est disponible, mais n'a pas été déployé par l'utilisateur, rendant l'exploitation de la vulnérabilité possible.*

- 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.

Ainsi, **les attaques par rançongiciel** ou **hameçonnage** tendent désormais à **cibler l'ensemble du tissu économique et social**.

Selon le panorama de la cybermenace 2023 de l'Anssi, ces attaques ont **augmenté de 30 % entre 2022 et 2023** avec **143 signalements d'attaque par rançongiciel en 2023**[1] en exploitant les faiblesses techniques ou les mauvaises pratiques des entités ciblées.

Comme le montre le schéma ci-dessous, **34 % de ces attaques visaient des TPE/PME**, **24 % des collectivités territoriales** (entre janvier 2022 et juin 2023, l'Anssi a traité en moyenne dix attaques par mois contre une collectivité), **10 % des établissements de santé** et **9 % des établissements d'enseignement supérieur**.

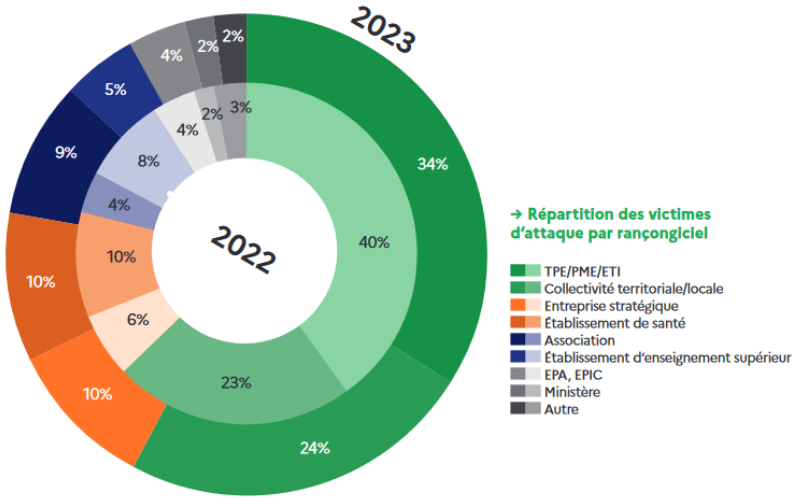
Les conséquences de ces attaques peuvent être **particulièrement pénalisantes pour les entités attaquées**, ainsi que pour **leurs usagers** ou **leurs clients**, voire **provoquer des faillites** ou **mettre des vies en danger**.

Citons à cet égard l'exemple de **l'attaque subie en août 2022 par le Centre hospitalier sud francilien**, victime d'une attaque par rançongiciel revendiquée par le groupe cybercriminel *Lockbit*, qui a entraîné **l'exfiltration de près de 11 gigaoctets de données médicales et personnelle**s et a **fortement perturbé le fonctionnement des services hospitaliers** pendant de longs mois.

Toujours dans le domaine de la santé, peuvent également être citées **les attaques subies en avril 2023 par le centre hospitalier de Bourg-en-Bresse** et **en octobre 2024 par le groupe Hospi Grand Ouest**, qui a entraîné **la déprogrammation de plusieurs opérations**.

Répartition des victimes d'attaques par rançongiciel

[1] *Cette tendance se limite toutefois aux incidents signalés à l'ANSSI ou ayant fait l'objet d'un dépôt de plainte, et ne constitue pas une vision exhaustive.*



Source : Panorama de la cybermenace 2023 de l'ANSSI

Ces attaques 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.

Notons enfin que **cette hausse des attaques criminelles** n'empêche nullement **le maintien à un niveau toujours très élevés des menaces de**

nature étatique, alors que le contexte géopolitique est aujourd'hui particulièrement perturbé.

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

Face à **l'évolution de la menace** et **à l'ampleur de ses conséquences**, les États membres de l'Union européenne, dont la France, ont jugé qu'il était **impératif de moderniser le cadre juridique** et se sont mobilisés en ce sens dès 2020, ce qui a conduit à **l'adoption de la directive NIS 2** à la fin de l'année 2022, pendant la présidence française de l'Union européenne (PFUE).

Si la cybermenace est susceptible de **toucher tous les acteurs de la vie économique et sociale**, il importe de garantir **une proportionnalité de traitement dans les obligations en matière de cybersécurité** mises à la charge des différentes entités qui ont vocation à être régulées.

À cette fin, 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).

L'article 3 de la directive NIS 2 prévoit qu'aux fins de cette directive, **les entités suivantes sont considérées comme étant des entités « essentielles »**.

Il s'agit en premier lieu **des entités appartenant à un secteur « hautement critique »** (visé par l'annexe I de la directive) qui **dépassent les plafonds applicables aux moyennes entreprises** prévus aux paragraphe 1 de l'article 2 de l'annexe de la recommandation 2003/361/CE, lequel dispose que « *La catégorie des micro, petites et moyennes entreprises (PME) est constituée des entreprises qui* ***occupent moins de 250 personnes*** *et dont* ***le chiffre d'affaires annuel n'excède pas 50 millions d'euros*** *ou dont* ***le total du bilan annuel n'excède pas 43 millions d'euros*** ».

Il s'agit en deuxième lieu **des prestataires de services de confiance qualifiés** et **des registres de noms de domaine de premier niveau** ainsi que **les fournisseurs de service DNS**, quelle que soit leur taille.

Sont également concernés **les fournisseurs de réseaux publics de communications électroniques** ou **de services de communications électroniques accessibles au public** qui constituent **des moyennes entreprises** en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE, lequel dispose que sont des moyennes entreprises celles qui **emploient au moins 50 personnes** et **dont le chiffre d'affaires annuel** ou **le total du bilan annuel excèdent chacun 10 millions d'euros**.

Sont enfin concernées **les entités de l'administration publique**, c'est-à-dire, conformément aux dispositions du f du 2 de l'article 2 de la directive :

- **des pouvoirs publics centraux** tels qu'ils sont définis par un État membre conformément au droit national ;
- ou **au niveau régional**, tel qu'il est défini par un État membre conformément au droit national, qui, à la suite d'une évaluation basée sur les risques, **fournit des services** dont **la perturbation** pourrait avoir **un impact important sur des activités sociétales ou économiques critiques**.

Le 5 de l'article 2 de la directive précise que les États membres peuvent prévoir que la directive s'applique :

- **aux entités de l'administration publique au niveau local** ;
- **aux établissements d'enseignement**, en particulier **lorsqu'ils mènent des activités de recherche critique**.

Le 7 de l'article 2 de la directive indique que cette dernière **ne s'applique pas aux entités de l'administration publique** qui exercent leurs activités dans **les domaines de la sécurité nationale**, **de la sécurité publique**, **de la défense** ou **de l'application de la loi**, y compris l**a prévention et la détection des infractions pénales**, ainsi que **les enquêtes et les poursuites en la matière**.

Le 8 de l'article 2 de la directive prévoit que les États membres peuvent **exempter des entités spécifiques** qui exercent des activités dans **les domaines de la sécurité nationale**, **de la sécurité publique**, **de la défense** ou **de l'application de la loi**, y compris **la prévention et la détection des infractions pénales**, ainsi que **les enquêtes** et **les poursuites en la matière**, ou qui fournissent **des services exclusivement aux entités de l'administration publique** des obligations prévues aux articles 21 et 23 de la directive en ce qui concerne ces activités ou services.

II. Le dispositif envisagé – Seront considérées notamment comme des entités essentielles les entreprises d'une taille significative appartenant à un secteur hautement critique mais également de nombreuses administrations de l'État et collectivités territoriales

Transposant les dispositions des articles 2 et 3 de la directive NIS 2, le présent article 8 établit **la liste des entités considérées comme « essentielles »** du point de vue **de la sécurité des systèmes d'information**, ces entités ayant vocation à **se voir imposer un certain nombre d'obligations** sous le contrôle de l'Anssi.

Selon cette dernière, ces entités « essentielles », qui devront respecter un niveau d'exigence plus élevées que les entités « importantes » définies à l'article 9, sont **des structures déjà sensibilisées ou confrontées à la menace cyber**.

D'autres, au regard de leur taille et de leur secteur d'activité, présentent **une forte dépendance aux infrastructures numériques**.

1) Les entreprises considérées comme des entités « essentielles » devront appartenir à un secteur hautement critique et obéir à un critère de taille significative

Le 1° prévoit que **sont considérées comme des entités « essentielles »** les entreprises appartenant à **un des secteurs d'activité « hautement critiques » qui emploient 250 personnes** ou **dont le chiffre d'affaires annuel excède 50 millions d'euros** et **dont le total du bilan annuel excède 43 millions d'euros**.

Le 2° y inclut **les établissements publics à caractère industriel et commercial (EPCI)** et **les régies dotées de la seule autonomie financière chargées d'un service public industriel et commercial** appartenant à un des secteurs d'activité « hautement critiques », qui emploient **au moins 250 personnes** ou dont **les produits d'exploitation excèdent 50 millions d'euros** et **le total du bilan annuel excède 43 millions d'euros**.

Dans le cas du 1° et du 2°, c'est donc 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**.

Comme rappelé *supra*, l'article 3 de la directive dispose que **sont des entités « essentielles »** les entités appartenant à un secteur « hautement critique » qui **dépassent les plafonds applicables aux moyennes entreprises** prévus aux paragraphe 1 de l'article 2 de l'annexe de la recommandation 2003/361/CE, lequel dispose que « *La catégorie des micro, petites et moyennes entreprises (PME) est constituée* ***des entreprises qui occupent moins de 250 personnes*** *et dont* ***le chiffre d'affaires annuel n'excède pas 50 millions d'euros*** *ou dont* ***le total du bilan annuel n'excède pas 43 millions d'euros*** ».

Ainsi, le projet de loi formule **une proposition contraposée de la définition de l'article 2 de l'annexe de la recommandation 2003/361/CE** afin de viser toutes les entreprises qui excèdent les critères des PME donc qui dépassent les seuils fixés :

- « moins de 250 personnes » devient « **au moins 250 personnes** » ;
- pour le chiffre d'affaires annuel, « n'excède pas » devient « **excède 50 millions d'euros** » ;
- pour le bilan annuel, « n'excède pas » devient « **excède 43 millions d'euros** » ;

- le « et » du nombre d'employés devient un « ou » et le « ou » du chiffre d'affaires et du bilan annuel devient un « et » afin d'intégrer, comme prévues par la directive et la recommandation de 2003, **des entreprises pouvant avoir un nombre d'employés inférieur à 250 personnes** mais **dont le chiffre d'affaires et le bilan annuel justifient leur régulation par la directive NIS 2**.

Si les rapporteurs comprennent le choix de proposer **une définition positive des critères de taille** permettant d'établir si une entreprise est ou non **une entité « essentielle »**, ils ne peuvent que constater que le choix initial de faire référence dans l'article 3 de la directive à la définition de l'article 2 de l'annexe de la recommandation 2003/361/CE créée **énormément de confusion**, car celui-ci ne permet pas de savoir quelles sont les entreprises entités « essentielles » mais seulement quelles sont les entreprises en deçà des seuils permettant de les qualifier d' « essentielles ».

Il aurait été **nettement préférable** de proposer directement **une définition positive** comme le fait le projet de loi de transposition.

Le 3° rajoute **les opérateurs de communications électroniques** qui emploient **au moins 50 personnes ou** dont le chiffre d'affaires annuel **et** le total du bilan annuel **excèdent chacun 10 millions d'euros**.

Le 4° dispose que **les prestataires de service de confiance qualifiés** sont considérés comme des entités « essentielles ».

C'est aussi le cas au 5° **des offices d'enregistrement**, c'est-à-dire des entités auxquelles **un domaine de premier niveau spécifique a été délégué** et qui est **responsable de l'administration de ce domaine**, y compris de l'enregistrement des noms de domaine en relevant et de son fonctionnement technique, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution de ses fichiers de zone sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage.

C'est enfin le cas des au 6° **des fournisseurs de services de systèmes de noms de domaine**.

Les entités visées aux 3° à 6° de l'article 8 sont effectivement toutes visées également par les dispositions de l'article 3 de la directive, ce qui témoigne **d'une transposition fidèle**.

Au total, selon l'Anssi, **quelque 2 000 entreprises privées devraient ainsi être considérées comme des entités « essentielles »** au titre du présent projet de loi.

2) <u>Les administrations considérées comme des entités « essentielles » incluront, sur choix de la France, de très nombreuses collectivités territoriales et leurs établissements publics</u>

La définition du **périmètre des administrations considérées comme des entités « essentielles »**, prévue au 7° de l'article 8, constitue un véritable choix opéré au niveau national dans le projet de loi, puisque la directive NIS 2, au paragraphe 5 de son article 2, laisse à chacun des États membres la possibilité de définir lui-même quelles « ***entités de l'administration publique au niveau local*** » **seront ou non concernées par le périmètre des obligations prévues par elle**, et, par conséquent, par le titre II du projet de loi.

Le point a) prévoit que sont considérées comme des entités « essentielles » **les administrations de l'État** et **leurs établissements publics administratifs**, à l'exception :

- **des administrations de l'État** qui exercent leurs activités dans les domaines **de la sécurité publique**, **de la défense** et **de la sécurité nationale**, **de la répression pénale** et **des missions diplomatiques et consulaires françaises** pour leurs réseaux et systèmes d'information ;
- **de leurs établissements publics administratifs** qui exercent leurs activités dans les mêmes domaines.

Cette exclusion des administrations régaliennes est effectivement **prévue** par les dispositions du 7 de l'article 2 de la directive NIS 2.

Toutefois, l'article 14 du projet de loi prévoit que ces administrations se verront appliquer **des mesures équivalentes**, **à l'exception du principe de remontée d'information au niveau européen** prévu par la directive afin d'assurer **la protection des informations confidentielles**.

Ce choix de transposition permet d'une part d'assurer **un niveau de protection au moins équivalent à ces administrations sensibles**, même si elles sont exclues par définition du champ de la régulation européenne, et d'autre part **garantit l'unicité des règles applicables à l'ensemble des administrations de l'État**.

Ne seront pas non plus considérées comme des entités essentielles :

- **les administrations de l'État** et **leurs établissements publics administratifs** qui sont désignés **entités « importantes »** (et non pas « essentielles ») par arrêté du Premier ministre, c'est-à-dire qui relèvent des dispositions de l'article 9 du projet de loi ;
- **les établissements publics administratifs de l'État** qui, compte tenu du faible impact économique et social de leur activité, **ne sont pas soumis à la présente loi** ; ces établissements publics sont désignés par arrêté du Premier ministre, dans des conditions précisées par décret en Conseil d'État.

Les points b), e), f) et g) prévoient, et c'est là **un choix particulièrement important et structurant**, que sont considérées comme **des**

entités « essentielles » qui se verront appliquer les obligations au titre de la cybersécurité prévues par le titre II du présent projet de loi :

- **les régions**, conformément aux dispositions de la directive qui visent expressément **les administrations au niveau régional** comme relevant d'un secteur hautement critique ;
- **les départements** ;
- **les communautés urbaines**, **les communautés d'agglomération** et **les métropoles** ;
- **les communes d'une population supérieure à 30 000 habitants** (ce qui représente moins de 1 % des communes) ;
- **leurs établissements publics administratifs** dont les activités s'inscrivent dans un des secteurs d'activité « hautement critiques » ou « critiques » ;
- **les syndicats de communes**[1], **les syndicats mixtes constitués exclusivement de communes et d'établissements publics de coopération intercommunale** et ceux composés uniquement **d'établissements publics de coopération intercommunale** et **les syndicats mixtes** de l'article L. 5721-2 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité « hautement critiques » ou « critiques » et dont **la population est supérieure à 30 000 habitants**, ce qui représente environ 38 % des EPCI ;
- **les institutions et organismes interdépartementaux** dont les activités s'inscrivent dans un des secteurs d'activité « hautement critiques » ou « critiques ».

Selon l'Anssi, **1 489 collectivités territoriales**, **groupements de collectivités territoriales** ou **organismes sous leur tutelle** devraient ainsi être considérés **comme des entités « essentielles »** au titre du présent projet de loi.

Ce choix d'intégrer les collectivités territoriales dans le champ d'application du texte s'explique par **les nombreuses attaques informatiques** qui ont affecté celles-ci au cours des dernières années.

Comme rappelé *supra*, en 2023, **les collectivités territoriales** ont représenté **24% des victimes d'attaques par rançongiciel** constatées par l'Anssi, avec **des conséquences parfois très significatives à l'échelle de ces collectivités** et **de leurs administrés**.

[1] *Le syndicat de communes est un établissement public de coopération intercommunale associant des communes en vue d'œuvres ou de services d'intérêt intercommunal.*

Les motifs qui poussent les cybercriminels à s'attaquer aux collectivités territoriales

- Importance des données : les collectivités détiennent une quantité importante de données sensibles sur leurs administrés (état civil, impôts, etc.) ;
- Infrastructure vieillissante : de nombreux systèmes d'information des collectivités sont anciens et trop peu sécurisés, ce qui facilite les intrusions ;
- Manque de ressources : les collectivités disposent souvent de budgets limités pour la cybersécurité, ce qui les empêche de mettre en place des mesures de protection suffisante ;
- Complexité des systèmes : les systèmes d'information des collectivités sont souvent complexes et interconnectés, ce qui les rend plus difficiles à sécuriser ;
- Insuffisance de personnel formé : le manque de personnel qualifié en cybersécurité complique la mise en œuvre et le maintien de dispositifs de sécurité efficaces.
- Manque de sensibilisation aux risques cyber : une insuffisante sensibilisation des élus, des agents et des citoyens aux risques cyber accroît la vulnérabilité face aux attaques.

Source : rapport IDATE

Ces dispositions visent à **intégrer dans le champ de la réglementation les collectivités territoriales** et **leurs activités les plus sensibles**, tout en conservant en dehors du champ d'application directe de la loi **la majorité des collectivités**, puisque **les communes de moins de 30 000 habitants** ne seront concernées, le cas échéant, que **par le biais de leur rattachement à une intercommunalité**.

Outre les collectivités elles-mêmes et leurs groupements, **les centres de gestion de la fonction publique territoriale**, mentionnés à l'article L. 452-1 du code général de la fonction publique, sont eux aussi désignés comme des entités « essentielles » en vertu du c) de l'article 8.

Le d) inclut également **les services départementaux d'incendie et de secours**, mentionnés à l'article L. 1424-1 du code général des collectivités territoriales.

Le h), enfin, inclut **les autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif à compétence nationale**, à l'exception de ceux qui sont désignés entité « importante » par arrêté du Premier ministre.

À noter que, dans un souci de proportionnalité, le Premier ministre désigne par arrêté **les organismes et personnes morales** qui, compte tenu du faible impact économique et social de leur activité, **ne sont pas soumis à la présente loi**, dans des conditions précisées par décret en Conseil d'État.

3) Les opérateurs qui étaient déjà couverts par la directive NIS 1, à savoir les OIV et les OSE, resteront logiquement couverts par les dispositions du présent projet de loi transposant NIS 2

En toute logique, l'article 8 dispose que les entités qui étaient **déjà assujetties à des obligations en matière de cybersécurité** sur le fondement de **la directive NIS 1** seront considérées comme **des entités « essentielles »** au titre du présent projet de loi.

Le 8° prévoit ainsi que sont des entités « essentielles » **les opérateurs d'importance vitale (OIV)** en tant qu'ils exercent une activité qualifiée de service essentiel en application du deuxième alinéa du 1° du I de l'article L. 1332-2 du code de la défense.

C'est également le cas en vertu du 9° **des opérateurs de services essentiels (OSE)** désignés en application des dispositions de l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation du droit de l'Union européenne dans le domaine de la sécurité.

Pour mémoire, cet article 5 prévoyait qu'étaient considérés comme OSE *« les opérateurs, publics ou privés, offrant **des services essentiels au fonctionnement de la société ou de l'économie** et dont **la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information** nécessaires à la fourniture desdits services »*.

Ces OSE étaient désignés par un arrêté du Premier ministre.

La directive NIS 2 prévoit en effet à son article 3 la possibilité pour les États membres de **désigner en tant qu'entités « essentielles » les entreprises ayant reçu le statut d'OSE au titre de NIS 1**.

4) Les établissements d'enseignement supérieur menant des activités de recherche se verront, sous réserve qu'ils correspondent à certains critères, appliquer les dispositions de transposition de la directive NIS 2

La directive NIS 2, au point b du paragraphe 5 de son article 2, prévoit que **les établissements d'enseignement**, en particulier **lorsqu'ils mènent des activités de recherche critique**, peuvent être **inclus sur décision des États membres** dans **le périmètre des entités auxquelles s'applique la directive**.

Le projet de loi fait effectivement le choix de prévoit au 10° de l'article 8 que **les établissements d'enseignement menant des activités de recherche**, désignés par arrêté du Premier ministre dans des conditions précisées par décret en Conseil d'État, comme **des entités « essentielles »**.

Pour être désigné comme entité « essentielle », un établissement devra toutefois **être concerné par l'un des quatre critères** suivants prévus à l'article 10 du projet de loi, critères qui reprennent par ailleurs quasiment au mot près les critères définis par les points b à e du paragraphe 2 de l'article 2 de la directive NIS 2 :

- être **le seul prestataire sur le territoire national** d'un service qui est essentiel **au maintien du fonctionnement de la société** et **d'activités économiques critiques** ;
- une perturbation du service fourni par cet établissement pourrait avoir **un impact important sur la sécurité publique**, **la sûreté publique** ou **la santé publique** ;
- une perturbation du service fourni par l'établissement pourrait induire **un risque systémique important**, en particulier pour les secteurs où **cette perturbation pourrait avoir un impact transfrontière** ;
- l'établissement est critique en raison de **son importance spécifique au niveau national ou local** pour le secteur ou le type de service concerné, ou pour d'autres secteurs interdépendants sur le territoire national.

De fait, comme le permet la directive NIS 2 et comme retenu par une majorité d'États membres, **les établissements d'enseignement menant des activités de recherche** ont été **inclus dans le champ d'application du projet de loi**.

L'objectif est de **protéger leurs activités particulièrement sensibles** et de **limiter les risques caractérisés** que **la menace cyber** fait notamment peser sur **leurs capacités d'innovation et leur sécurité**.

Ce choix s'explique aussi par le fait que, malgré leur sensibilité, ces entités ne sont aujourd'hui couvertes **par aucun cadre réglementaire contraignant** et qu'elles ont **besoin d'élever leur niveau de maturité en matière de cybersécurité**.

L'attaque contre l'université de Paris-Saclay en août 2024, qui a **perturbé la rentrée académique de l'établissement** en rendant **indisponibles plusieurs services numériques**[1], ou bien celle subie **par l'université Panthéon-Sorbonne** avec **le vol des données personnelles de milliers d'étudiants**, illustre **ce niveau élevé d'exposition à la menace cybercriminelle** et **la vulnérabilité** de ces établissements.

III. La position de la commission – le choix d'inclure un grand nombre de collectivités territoriales et les établissements d'enseignement supérieur est ambitieux mais nécessaire

L'aggravation de la menace cyber constitue **une réalité** à laquelle chacun est confronté et pèse désormais **sur l'ensemble des acteurs économiques et sociaux**.

---

[1] *L'établissement avait été contraint de couper des services informatiques sur l'ensemble du campus, dont les boîtes e-mails de ses enseignants et chercheurs, compliquant grandement la rentrée de septembre.*

Il est donc indispensable **d'élever le niveau général en matière de cybersécurité des systèmes d'information** afin de lutter contre **les faiblesses techniques** ou **les mauvaises pratiques** qu'exploitent **les acteurs hostiles** à des fins **d'espionnage stratégique** ou **industriel**, ou, de plus en plus, **des acteurs criminels** qui cherchent à **s'enrichir en utilisant des rançongiciels** ou **de l'hameçonnage**.

1) Les critères de taille font que le statut d'entité « essentielle » devrait être réservé à des entreprises suffisamment solides pour faire face au niveau d'exigence élevé auquel elles seront soumises

En ce qui concerne **les entreprises**, l'article 8 transpose fidèlement le texte de la directive en prévoyant que le statut d'entité « essentielle » sera réservé à **des entreprises de taille significative** appartenant à **des secteurs « hautement critiques »**, ce qui constitue une nécessité pour **assurer la proportionnalité des mesures de cybersécurité qui leur seront imposées**.

Il s'agit effectivement **d'adapter les exigences aux** menaces qui pèsent sur les entités mais également à **leur caractère plus ou moins critique** ainsi q**u'à leurs capacités effectives**. Cet enjeu de proportionnalité constitue vraisemblablement **le facteur clef de succès de la mise en œuvre du titre II de ce projet de loi** transposant la directive NIS 2, tant pour avoir **un niveau de protection adéquat** qu'en terme **d'acceptabilité des exigences**.

Quoi qu'il en soit, selon les estimations du cabinet de conseil Idate, le coût de l'application de la directive NIS 2 devrait représenter **environ 2 milliards d'euros pour les entreprises française** en comptant à la fois **le coût de la mise en conformité et celui du recrutement d'experts**. Les 12 000 entreprises de taille moyenne, qui seront pour l'essentiel classées comme entités « importantes » (voir le commentaire de l'article 9), devraient y consacrer près de **1,3 milliards d'euros**, ce qui implique donc **une charge de 700 millions d'euros** pour les 2 000 entreprises classées entités « essentielles », lesquelles disposent pourtant souvent déjà **d'une réelle maturité cyber**.

Ces coûts devront être mis en relation avec **les indéniables avantages à long terme qu'en retireront les entreprises** : r**éduction de la probabilité de pertes financières liées aux attaques cyber**, grâce notamment à la limitation des dommages qui permettra de réduire les coûts de reprise, **amélioration de la réputation de l'entreprise vis-à-vis de ses partenaires et clients**, etc.

2) Le choix d'inclure dans le périmètre des entités régulées les collectivités territoriales est un choix fort mais nécessaire

Si elle est naturellement très attentive à ce que **les obligations mises à la charge des collectivités territoriales** et **de leurs établissements publics** soient également **proportionnées** et **pleinement justifiées**, la commission spéciale **approuve et soutient le choix politique** consistant à **inclure dans le texte en tant qu'entités « essentielles » de très nombreuses collectivités territoriales infrarégionales**.

Eu égard à **l'importance des services publics rendus à nos concitoyens par les collectivités territoriales et leurs établissements publics** et à **l'ampleur des perturbations que peuvent engendrer les cyberattaques** (services perturbés, perte de données sensibles, dommages financiers, etc.), il est indispensable que **l'ensemble des collectivités** visées par le présent article 8 en tant qu'entités « essentielles » ou par l'article 9 en tant qu'entités « importantes » **fassent l'effort**, lorsque ce n'est pas déjà le cas, **d'élever leur niveau de cybersécurité** pour se **conformer aux obligations qui seront prévues par le référentiel dédié de l'Anssi**.

Car **les montant investis sont aujourd'hui insuffisants**. Les dépenses en solutions de cybersécurité représentent **en moyenne entre 4% et 8% des budgets informatique des collectivités**, alors qu'il faudrait que ces dépenses représentent **environ 10 % de ces budgets pour atteindre une protection de base** et **12 % pour se mettre au niveau requis par la directive NIS 2**.

Cet effort représentera toutefois **un coût très important** puisqu'un rapport du cabinet Idate rendu public au mois de novembre 2024 estime que **le coût pour l'ensemble des collectivités terr**itoriales **des solutions de sécurité nécessaires** à leur mise en conformité avec la directive NIS 2 s'élèverait à **690 millions d'euros par an**. S'y ajouteraient **105 millions d'euros par an au titre de l'embauche et de la formation de ressources humaines qualifiées**. Soit un total estimé à environ **795 millions d'euros par an**.

Ces lourdes dépenses d'investissement et de fonctionnement n'iront pas de soi, alors que, pour prendre l'exemple des départements, le représentant de l'Association des départements de France (ADF) indiquait devant la commission spéciale que les crédits dédiés à l'informatique pourraient être, en 2025, **amputés de l'ordre de 30 % à 50 % en moyenne dans la plupart de ces collectivités**.

Sur le plan humain, il sera nécessaire **de recruter et de former les agents disposant des compétences adéquates**. Or les collectivités territoriales sont confrontées sur le marché de l'emploi à la concurrence des acteurs privés.

En outre, même si l'ensemble des associations représentant les collectivités territoriales ont salué la concertation menée par l'Anssi depuis l'automne 2023, **un effort de communication très important vis-à-vis des collectivités territoriales demeure indispensable** puisque **23 % des 500 décideurs informatiques** interrogés dans la dernière édition du baromètre sur la maturité cyber des collectivités reconnaissaient n'avoir jamais entendu parler de la directive NIS 2 et **seuls 24 % d'entre eux se déclaraient prêts à appliquer ses mesures de transposition**. La marge de progression est donc importante, le manque de connaissances et de préparation patent.

3) <u>Les établissements d'enseignement supérieur doivent également être mieux protégés contre les menaces cyber</u>

Le second choix de transposition important proposé à l'article 8, et que **la commission spéciale approuve également**, est celui **d'inclure les**

établissements d'enseignement qui mènent des activités de recherche parmi **les entités régulées** par le titre II du présent projet de loi de transposition de la directive NIS 2.

Comme rappelé *supra,* **les attaques cyber subies par l'université de Paris-Saclay et par l'université Panthéon-Sorbonne en 2024** ont montré combien ces **établissements stratégiques pour l'enseignement et la recherche publique** constituent **des cibles de choix** pour les pirates cyber, qu'ils agissent à **des fins d'espionnage** ou **pour des motifs purement criminels**.

La commission a adopté cet article sans modification.

Article 9

Définition des entités « importantes » du point de vue de la sécurité des systèmes d'information

Cet article vise à définir la liste des entités considérées comme « importantes » du point de vue de la sécurité des systèmes d'information, c'est-à-dire devant faire l'objet de mesures de cybersécurité significatives mais néanmoins moins fortes, dans un souci de proportionnalité, que celles qui s'appliquent aux entités « essentielles » définies à l'article 8.

La commission a adopté cet article sans modification.

I. La situation actuelle – la directive NIS 2 propose une définition en creux des entités « importantes », en faisant référence aux critères applicables aux entités « essentielles »

Comme rappelé dans le commentaire de l'article 8, **la multiplication des cyberattaques** contre **de très nombreux acteurs de la vie économique et sociale** a conduit l'Union européenne, avec un rôle moteur de la France, à **adopter la directive NIS 2** visant à **renforcer les obligations en matière de cybersécurité de très nombreux acteurs**.

À cet égard, l'article 3 de la directive NIS 2 définit **les entités « essentielles »** qui se verront assigner **des obligations renforcées** et **les entités « importantes »** pour lesquelles ces obligations **seront moins exigeantes**, dans **un souci de proportionnalité**.

Le paragraphe 1 de l'article 3 de la directive précise les entités qui sont considérés comme « essentielles » et son paragraphe 2 définit, **en creux**, **les entités considérées comme « importantes »** : il s'agit des entités **appartenant à un secteur « hautement critique »** (annexe I de la directive) ou à **un secteur « critique »** (annexe II de la directive) qui ne constituent pas des entités « essentielles » en vertu du paragraphe 1.

Sont aussi considérées comme **« importantes »** les entités **identifiées en tant que telles par un État membre** en vertu de l'article 2, paragraphe 2, points b) à e), une disposition dont la transposition est assurée par l'article 10 du présent projet de loi.

II. Le dispositif envisagé – une transposition fidèle des dispositions de la directive, qui, là aussi, définit principalement en creux la notion d'entité « importante », et fait le choix d'inclure les communautés de commune et les établissements d'enseignement supérieur

Le présent article 9, qui assure la transposition du paragraphe 3 de l'article 2 de la directive NIS 2, établit **la liste des entités considérées comme « importantes »** du point de vue de **la sécurité des systèmes d'information**,

ces entités ayant vocation à se voir imposer **des obligations sous le contrôle de l'Anssi**, ces obligations étant toutefois **moins exigeantes** que celles pesant sur les entités considérées comme « essentielles » énumérées à l'article 8.

1) Des seuils d'application aux entreprises plus bas que ceux prévus à l'article 8 pour les entités « essentielles »

En premier lieu, le 1° de l'article 9 prévoit que sont **des entités « importantes » 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**.

À titre de comparaison, et pour mémoire, le 1° de l'article 8 prévoit pour sa part que sont considérées comme des entités « essentielles » les entreprises **appartenant à un des secteurs d'activité « hautement critiques »** qui **emploient 250 personnes** ou dont **le chiffre d'affaires annuel excède 50 millions d'euros** et **dont le total du bilan annuel excède 43 millions d'euros**.

Les différences entre les deux catégories portent donc sur les critères suivants :

- alors qu'une entreprise ne sera une entité « essentielle » que si elle appartient à un secteur « hautement critique », elle peut être considérée comme **une entité « importante »** qu'elle appartienne à un secteur **« hautement critique »** ou seulement **« critique »** ;
- **les seuils sont plus bas** pour être considéré comme **une entité « importante »**. Il faut employer **au moins 50 personnes** contre 250 personnes pour une entité « essentielle ». Alternativement, il faut disposer **d'un chiffre d'affaires et d'un bilan annuel excédant chacun 10 millions d'euros**, contre respectivement **50 millions d'euros** et **43 millions d'euros** pour être reconnus comme une entité « essentielle ».

Cette classification est résumée dans le tableau ci-dessous qui **précise les critères applicables aux entreprises** en vertu des articles 8 et 9.

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

Là encore, le projet de loi formule **une proposition contraposée de la définition de l'article 2 de l'annexe de la recommandation 2003/361/CE** afin de viser toutes les entreprises qui excèdent les critères des PME donc qui dépassent les seuils fixés :

- « moins de 50 personnes » devient « **au moins 50 personnes** » ;
- pour le chiffre d'affaires annuel, « n'excède pas » devient « **excède 10 millions d'euros** » ;
- pour le bilan annuel, « n'excède pas » devient « **excède 10 millions d'euros** » ;
- le « et » du nombre d'employés devient un « ou » et le « ou » du chiffre d'affaires et du bilan annuel devient un « et » afin d'intégrer, comme prévues par la directive et la recommandation de 2003, **des entreprises pouvant avoir un nombre d'employés inférieur à 50 personnes** mais **dont le chiffre d'affaires et le bilan annuel justifient leur régulation par la directive NIS 2**.

Si les rapporteurs comprennent le choix de proposer **une définition positive des critères de taille** permettant d'établir si une entreprise est ou non **une entité « importante »**, ils ne peuvent que constater que le choix initial de faire référence dans l'article 3 de la directive à la définition de l'article 2 de l'annexe de la recommandation 2003/361/CE créée **énormément de confusion**, car celui-ci définit négativement ce que sont les micro, petites et moyennes entreprises[1] d'une part, et les petites entreprises d'autre part[2].

Il aurait été **nettement préférable** de proposer directement **une définition positive** comme le fait le projet de loi de transposition.

Le 8° prévoit également que, s'ils ne sont pas considérés comme des entités « essentielles », sont alors considérés comme **des entités « importantes » les établissements publics à caractère industriel et commercial (EPIC)** et l**es régies dotées de la seule autonomie financière chargées d'un service public industriel et commercial** appartenant à des secteurs d'activité « hautement critiques » ou « critiques », qui emploient **au moins 50 personnes** ou dont **le produit d'exploitation et le total du bilan annuel** excèdent chacun **10 millions d'euros**. Comme pour les entreprises, **les seuils sont plus bas** et les secteurs d'activité ne se limitent pas aux secteurs « hautement critiques », mais également aux secteurs « critiques ».

---

[1] *Définition de micro, petites et moyennes entreprises (PME) : les entreprises « qui occupent moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total du bilan annuel n'excède pas 43 millions d'euros ».*

[2] *Définition de petite entreprise : une entreprise « qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros ».*

2) Les autres entités « importantes » s'inscrivent largement en complément des entités qualifiées d'« essentielles » à l'article 8

L'article 8 définit d'autres entités comme **« importantes »** au titre des obligations prévues par le titre II du présent projet de loi, principalement par **des critères** qui s'appliquent **en creux** de ceux prévus à l'article 9 pour les entités dites « essentielles ».

Le 2° prévoit ainsi que **les opérateurs de communications électroniques** qui ne sont pas des entités « essentielles » sont par défaut **des entités « importantes »**. L'article 9 prévoyant que **les opérateurs de communications électroniques** qui emploient **au moins 50 personnes** ou dont **le chiffre d'affaires annuel et le total du bilan annuel excèdent chacun 10 millions d'euros** sont des entités « essentielles », cela signifie que **sont des entités « importantes » les opérateurs de communications électroniques** qui emploient **moins de 50 personnes** ou **dont le chiffre d'affaires annuel et le total du bilan annuel sont inférieurs**, au moins pour l'un des deux, **à 10 millions d'euros**.

Le 3° prévoit que **les prestataires de services de confiances** qui ne sont pas des entités « essentielles » sont **des entités « importantes »**. L'article 8 prévoyant que sont des entités « essentielles » les prestataires de service de confiance « qualifiés », cela signifie que **les prestataires de service de confiance qui ne sont pas « qualifiés » rentrent dans la catégorie des entités « importantes »**, dont les obligations au titre de la cybersécurité sont plus légères que celles qui s'appliquent aux entités « essentielles ».

Le 4° dispose que **les communautés de communes** et **leurs établissements publics administratifs** dont les activités s'inscrivent dans un des secteurs d'activité « hautement critiques » ou « critiques » sont **des entités « importantes »**.

Alors que sont considérés comme des entités « essentielles » les communautés urbaines, les communautés d'agglomération, les métropoles et les communes de plus de 30 000 habitants, **toutes les communautés de communes entrent ainsi dans le champ des entités « importantes »**.

Quant **aux communes de moins de 30 000 habitants**, c'est-à-dire l'immense majorité des communes françaises, elles ne seront concernées **pas concernées en elles-mêmes par les mesures de transposition de la directive NIS 2** mais le seront malgré tout **à travers leur intercommunalité de rattachement**.

En vertu du 5°, sont **des entités « importantes » les établissements d'enseignement menant des activités de recherche** qui ne sont pas des entités « essentielles ». Pour mémoire, l'article 8 prévoit que pour être classé comme « essentiel », **un établissement menant des activités de recherche doit être concerné par l'un des quatre critères prévus à l'article 10**.

S'il n'est concerné par aucun des quatre critères, il est considéré comme **une entité « importante »**, sauf à faire partie des établissements désignés par arrêté du Premier ministre **comme n'étant pas soumis à la présente loi compte tenu du faible impact économique et social de leur activité**. Les conditions dans lesquelles le Premier ministre procède à cette désignation par arrêté sont précisées par décret en Conseil d'État.

Le 6° de l'article 9 prévoit que **des établissements publics administratifs de l'État** peuvent être expressément désignés **en tant qu'entités « importantes »** par arrêté du Premier ministre, dans des conditions fixées en Conseil d'État.

Le Premier ministre, toujours dans des conditions fixées par décret en Conseil d'État, peut expressément désigner par arrêté en tant qu'entités « importantes **» les autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif à compétence nationale**.

III. La position de la commission – la nécessité d'imposer des obligations bien proportionnées aux entités « importantes » et clairement plus légères que celles qui seront exigées des entités « essentielles »

Lors de son audition, la ministre chargée du numérique a indiqué que **80 % des entités visées par la transposition de la directive NIS 2** assurée par le titre II du présent projet de loi seront **des entités « importantes »** au sens du présent article 8, ce qui devrait représenter **environ 12 000 entités**.

Dans un souci de **proportionnalité** qui doit conduire à tenir compte **de leur taille**, **de leurs moyens financiers et humains**, mais également **de leur caractère moins critique** que les entités « essentielles », ces entités « importantes » se verront imposer, selon le directeur général de l'Anssi entendu par la commission spéciale, **des mesures de sécurité d'« *hygiène numérique* »** afin de les aider à **prendre pleinement conscience des enjeux de cybersécurité** et de **l'impact particulièrement dommageable** que **les cyberattaques pourraient avoir sur leurs activités**.

De fait, si elles n'ont **pas vocation à être protégées contre la menace stratégique ciblée d'un service de renseignements étranger**, ces entités sont **les victimes récurrentes**, pour ne pas dire quotidiennes, **d'une menace systémique**.

Selon l'Anssi, **le niveau d'exigence requis vis-à-vis de ces entités**, et qui sera détaillé dans le référentiel mentionné à l'article 14, sera conçu pour **diminuer la probabilité qu'elles soient atteintes par un rançongiciel courant**, sans nécessiter **des investissements disproportionnés**.

Le directeur général de l'Anssi a ainsi expliqué à la commission spéciale que son objectif serait **d'accompagner au mieux ces entités** en leur

recommandant **des mesures de sécurité adaptées aux obligations prévues par la directive** ainsi qu'à **leur niveau de maturité cyber**.

Cette approche devra permettre de **munir les plus fragiles de ces entités d'un filet de sécurité cyber minimal**. De fait, la question n'est plus tant aujourd'hui de savoir **si une entité sera attaquée un jour**, mais plutôt **quand elle le sera si elle n'a pas fait le nécessaire pour se protéger**. Or, en matière de cybersécurité, il est souvent estimé que **le coût de la sécurité est cent fois inférieur au coût d'une attaque réussie**.

Selon le directeur général de l'Anssi, pour de petites structures partant de zéro - ce n'est pas le cas de toutes -, l'investissement initial demandé serait de l'ordre de **100 000 à 200 000 euros**, **les frais récurrents représentant 10 % de la somme mobilisée au départ**.

Sur la question des contrôles, les entités « importantes » se verront appliquer **un régime de supervision uniquement *ex post***, qui pourra être déclenché par tout élément de preuve ou toute information portée à l'attention de l'Anssi, alors que **le régime de supervision des entités essentielles sera à la fois *ex ante* et *ex post***.

En ce qui concerne **les sanctions**, l'amende applicable aux entreprises entités « importantes » **ne pourra excéder 7 millions d'euros** ou **1,4 % du chiffre d'affaires annuel mondial total**, hors taxes, de l'exercice précédent de l'entreprise, le montant le plus élevé étant retenu, contre respectivement **10 millions d'euros** et **2% du chiffres d'affaires annuel mondial** pour les entités « essentielles ».

Il faudra toutefois que ce dispositif de sanction **ne soit pas mis en œuvre pendant les trois ans qui suivront la promulgation de la présente loi**, afin que les entités régulées **aient le temps de mettre en place les mesures requises**.

Ainsi, **la différence de traitement entre entités « essentielles »**, souvent déjà **très matures en termes de cybersécurité**, et **entités « importantes »**, qui le sont **parfois beaucoup moins**, devrait être **nette** et **bien respecter le principe de proportionnalité** qui doit guider l'action du législateur, du pouvoir réglementaire puis de l'Anssi dans sa pratique opérationnelle.

Dans le cas des quelque **992 communautés de communes** que compte notre pays et **de leurs établissements publics administratifs**, qualifiés d'entités « importantes » par le présent article 8, la cybersécurité constitue **une préoccupation majeure**, entretenue par **la récurrence des cyberattaques**.

Pour autant, leurs responsables craignent de se voir imposer **des obligations trop exigeantes** alors qu'elles **manquent souvent de moyens** et auront besoin **d'un accompagnement très soutenu de la part de l'État**, sachant par ailleurs qu'elles rencontrent déjà et continueront à rencontrer **des difficultés en termes de ressources humaines** ou **de recours aux prestataires**

privés en matière cyber. Il sera par exemple nécessaire de clarifier si les communautés de communes devront disposer d'un responsable de la sécurité des systèmes d'information (RSSI) ou si **un simple référent en cybersécurité** pourra suffire.

Il sera donc essentiel que l'Anssi prenne **toute la mesure des réalités de terrain**, parfois très diverses, **des communautés de commune**.

La commission a adopté cet article sans modification.

Article 10

Autres entités susceptibles d'être désignées comme entités « essentielles » ou « importantes » du point de vue de la sécurité des systèmes d'information par arrêté du Premier ministre

Cet article vise à transposer des dispositions de l'article 2 de la directive NIS 2, qui prévoit d'assujettir sans condition de taille des entités appartenant aux secteurs « hautement critiques » ou « critiques », dès lors que la perturbation de leur service par une attaque cyber pourrait avoir un impact important pour le fonctionnement de la société, de secteurs économiques critiques, pour la sécurité publique, la sûreté publique, la santé publique ou bien encore pourrait représenter un risque systémique.

La commission a adopté cet article sans modification.

I. La situation actuelle – la directive NIS 2 définit les cas dans lesquels des entités peuvent être qualifiées d'« essentielles » ou « importantes » quelle que soit leur taille

L'article 2 de la directive NIS 2 relatif à son « Champ d'application » prévoit aux points b à e de son paragraphe 2 que **la directive s'applique aux entités** d'un type visé à l'annexe I (secteur d'activité « hautement critique ») ou à l'annexe II (secteur d'activité « critique »), **quelle que soit leur taille**, lorsque :

- l'entité est, dans un État membre, **le seul prestataire d'un service** qui est **essentiel** au maintien **d'activités sociétales** ou **économiques critiques** ;
- **une perturbation** du service fourni par l'entité pourrait avoir **un impact important sur la sécurité publique**, **la sûreté publique** ou **la santé publique** ;
- **une perturbation** du service fourni par l'entité pourrait induire **un risque systémique important**, en particulier pour les secteurs où cette perturbation pourrait avoir **un impact transfrontière** ;
- l'entité est **critique** en raison de **son importance spécifique au niveau national ou régional** pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre.

II. Le dispositif envisagé – le Premier ministre pourra désigner par arrêté une entité comme « essentielle » ou « importante », dès lors qu'elle remplir certains critères, même si elle n'est pas couverte par les dispositions des articles 8 et 9 du présent projet de loi

En complément des dispositions de l'article 8, qui prévoit la liste des entités « essentielles » du point de vue de la cybersécurité, et de celles de l'article 9, qui prévoit la liste des entités « importantes », l'article 10 introduit

la possibilité pour le Premier ministre de **désigner par arrêté** comme **entité « essentielle »** ou comme **entité « importante »** une entité exerçant une activité relevant **d'un secteur d'activité « hautement critique »** ou **« critique »**, **quelle que soit sa taille**, sous réserve de justifier cette désignation au regard de **l'un des quatre critères suivants**.

Le 1° prévoit que le Premier ministre peut ainsi désigner comme entité « essentielle » ou « importante » une entité qui serait **le seul prestataire sur le territoire national** d'un service qui est **essentiel au fonctionnement de la société** et **d'activités économiques**.

Le 2° dispose qu'une telle désignation peut intervenir si une perturbation du service fourni par l'entité pourrait avoir **un impact important sur la sécurité publique**, **la sûreté publique** ou **la santé publique**.

Le 3° introduit le critère selon lequel une perturbation du service fourni par l'entité pourrait induire **un risque systémique important**, en particulier pour les secteurs où cette perturbation pourrait avoir **un impact transfrontalier**.

Le 4°, enfin, prévoit que le Premier ministre peut désigner comme une entité « essentielle » ou « importante » **une entité critique en raison de son importance spécifique au niveau national ou local** pour le secteur ou le type de service concerné, ou pour d'autres secteurs interdépendants du territoire national.

Ces 1° à 4° **reprennent très précisément** les points b à e du paragraphe 2 de l'article 2 de la directive NIS 2, assurant ainsi **la transposition de ces dispositions**.

III. La position de la commission – une transposition fidèle de dispositions de l'article 2 de la directive NIS 2

L'article 10 constitue **une transposition fidèle d'une partie des dispositions de l'article 2 de la directive NIS 2**, qui prévoit d'assujettir **sans condition de taille** des entités appartenant aux secteurs « hautement critiques » ou « critiques », dès lors que **la perturbation de leur service par une attaque cyber** pourrait avoir **un impact important pour le fonctionnement de la société**, **de secteurs économiques critiques**, pour **la sécurité publique**, **la sûreté publique**, **la santé publique** ou bien encore pourrait représenter **un risque systémique**.

Le pouvoir de désignation de ces entités par arrêté est **attribué au Premier ministre**, tutelle de l'Anssi, ce qui permettra à celle-ci de recenser puis de lui proposer la liste de tous les opérateurs concernés.

Lors des auditions menées par la commission spéciale, plusieurs intervenants ont demandé **la mise en place d'une voie de recours spécifique** en cas de contestation par une entité de son classement comme « essentielle » ou « critique » par arrêté du Premier ministre.

La mise en place d'une telle voie de recours n'est nullement nécessaire, les entités en question ayant la possibilité, en cas de contestation, de former **un recours gracieux** puis, le cas échéant, **un recours contentieux** devant la justice administrative.

En outre, il convient de rappeler que la désignation d'une entité comme « essentielle » ou « importante » du point de vue de la cybersécurité sur le fondement du présent article 10 par le Premier ministre **ne constitue nullement une sanction**, et qu'il ne s'agit **pas non plus de mettre à sa charge des obligations pour la pénaliser**, mais bien de tenir compte de son importance particulière pour le fonctionnement de secteurs prioritaires de la vie de la Nation, ce qui rend nécessaire la mise en place d'un niveau de cybersécurité suffisant.

La commission a adopté cet article sans modification.

Article 11

Compétence et territorialité des dispositions du titre II sur la sécurité des systèmes d'information

Cet article vise à définir les règles de compétences des États membres pour l'application des dispositions de la directive avant tout par des critères territoriaux.

La commission a adopté cet article sans modification.

I. La situation actuelle – la directive NIS 2 définit les compétences des États membres pour son application avant tout par des critères territoriaux

L'article 26 de la directive NIS 2 définit **les règles de compétences des États membres** pour **l'application des dispositions de la directive**, avant tout par **des critères territoriaux**.

Son paragraphe 1 prévoit ainsi que les entités relevant du champ d'application de la directive sont considérées comme **relevant de la compétence de l'État membre dans lequel elles sont établies**.

Font toutefois exception les cas suivants :

- au point a du paragraphe 1, il est prévu que les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public sont considérés comme **relevant de la compétence de l'État membre dans lequel ils fournissent leurs services** ;

- au point b du paragraphe 1, il est prévu que les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux sont considérés comme **relevant de la compétence de l'État membre dans lequel ils ont leur établissement principal dans l'Union** ;

- au point c du paragraphe 1, il est prévu que les entités de l'administration publique sont considérées comme **relevant de la compétence de l'État membre qui les a établies**.

Le paragraphe 2 de l'article 2 de la directive prévoit qu'une entité visée au point b du paragraphe 1 (les fournisseurs de service DNS, etc.) est considérée avoir **son établissement principal dans l'Union et dans l'État membre où sont principalement prises les décisions relatives aux mesures de gestion des risques de cybersécurité**.

Si un tel État membre ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union, l'établissement principal est considéré comme **se trouvant dans l'État membre où les opérations de cybersécurité sont effectuées**.

Si un tel État membre ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre **où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union**.

Le paragraphe 3 de l'article 26 de la directive prévoit que si une entité visée au point b) du paragraphe 1 n'est pas établie dans l'Union mais offre des services dans l'Union, **elle désigne un représentant dans l'Union**.

Le représentant est établi dans l'un des États membres dans lesquels les services sont fournis. Une telle entité est considérée comme **relevant de la compétence de l'État membre dans lequel le représentant est établi**.

En l'absence de désignation d'un représentant dans l'Union, tout État membre dans lequel l'entité fournit des services peut **intenter une action en justice contre l'entité pour violation de la directive**.

II. Le dispositif envisagé – une transposition fidèle des dispositions relatives aux modalités d'application territoriale des obligations prévues par la directive NIS 2

L'article 11 porte sur **les modalités d'application territoriale** des dispositions du titre II sur la sécurité des systèmes d'information et assure **une transposition fidèle des dispositions de l'article 26 de la directive NIS 2**.

Son I pose les règles relatives aux entités « essentielles » et aux entités « importantes » définies sur le fondement des articles 8, 9 et 10 du projet de loi.

Pour que le titre II s'applique à ces entités, le 1° du I prévoit qu'il faut que celles-ci soient **établies sur le territoire national**, reprenant en cela la règle de principe posée par le paragraphe 1 de l'article 26 de la directive.

En vertu du 2°, il faut, s'agissant des opérateurs de communications électroniques, **qu'ils fournissent leurs services sur le territoire national**, ce qui est conforme au point a) du paragraphe 1 de l'article 26 de la directive.

Celui-ci prévoit effectivement que pour les fournisseurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques accessibles au public, **c'est le critère de la fourniture des services qui est déterminant**. Ainsi, pour ce type d'opérateur, **peut relever de la compétence distincte et concurrente de plusieurs États membres** une entité « essentielle » ou « importante » **qui fournit des services dans différents États membres**.

En vertu du 3°, il faut, s'agissant des fournisseurs de services de système de noms de domaine, des offices d'enregistrement, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux :

- **qu'ils aient leur établissement principal sur le territoire national**.

S'agissant de ces acteurs numériques, le b) du paragraphes 2 de l'article 26 de la directive NIS 2 prévoit effectivement que ces entités relèvent de la compétence **d'un seul État membre**, à savoir **celui de l'établissement principal** ;

- ou, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national, **qu'ils aient désigné un représentant établi sur le territoire national**.

Le paragraphe 3 de l'article 26 de la directive prévoit effectivement que si une entité visée au point b) du paragraphe 1 n'est pas établie dans l'Union mais offre des services dans l'Union, **elle désigne un représentant dans l'Union**. Le représentant est établi **dans l'un des États membres** dans lesquels les services sont fournis. Une telle entité est considérée comme **relevant de la compétence de l'État membre dans lequel le représentant est établi**.

Les conditions d'établissement sur le territoire national ne s'appliquent pas aux administrations et établissements publics. Ceux-ci sont effectivement considérés comme **relevant de la compétence de l'État membre qui les a établies**, conformément au c) de l'article 26 de la directive.

Le II de l'article 11 dispose que s'agissant **des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers**, les obligations du titre II concernent :

- ceux qui ont **leur établissement principal sur le territoire national** ;
- ou ceux qui ont désigné **un représentant établi sur le territoire national**, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national.

Là encore, il s'agit d'un dispositif conforme aux dispositions des paragraphes 1 et 2 de l'article 26 de la directive.

Le III de l'article 11 précise enfin que pour l'application des I et II, l'établissement principal s'entend du lieu :

- où sont principalement prises **les décisions relatives aux mesures de gestion des risques en matière de cybersécurité** ;

- ou, à défaut, **le lieu où les opérations de cybersécurité sont effectuées** ;

- ou, à défaut, **l'établissement comptant le plus grand nombre de salariés dans l'Union européenne**.

Les dispositions de ce III sont **conformes** aux critères énoncés au paragraphe 2 de l'article 26 de la directive NIS 2 qui prévoit effectivement que les entités visées au b du paragraphe 1 (les fournisseurs de services DNS, etc.) **relèvent de la compétence d'un seul État membre**, à savoir **celui de l'établissement principal**.

Toutefois, ces critères semblent ici s'appliquer à l'ensemble des entités visées par l'article 26 de la directive et l'article 11 du présent projet de loi, alors que le texte de l'article 26 de la directive porte bien **uniquement sur les entités visées au b du paragraphe 1**.

III. La position de la commission – une transposition très fidèle des dispositions de l'article 26 de la directive NIS 2

L'article 11 du projet de loi constitue **une transposition très fidèle et souvent littérale des dispositions de l'article 26 de la directive NIS 2,** qui établit **les compétences des différents États membres** sur **les entités auxquelles s'appliquent les dispositions de la directive**. Il n'appelle donc pas de commentaires particuliers de la commission spéciale.

La commission a adopté sans modification cet article ainsi modifié.

Article 12

Enregistrement des entités « essentielles » et « importantes » auprès de l'autorité nationale de sécurité des systèmes d'information

Cet article prévoit que l'autorité nationale de sécurité des systèmes d'information établit et met à jour la liste des entités « essentielles », des entités « importantes » et des bureaux d'enregistrement sur la base des informations que ces entités et bureaux d'enregistrement lui communiquent.

La commission a adopté l'article 12 modifié par deux amendements prévoyant :

- la nécessité d'une mise à jour au minimum tous les deux ans de la liste des entités régulées par le titre II du projet de loi transposant la directive NIS 2, telle que prescrit par la directive ;

- que le décret en Conseil d'État pris pour l'application de cet article fait l'objet d'un avis de la commission nationale de l'informatique et des libertés.

I. La situation actuelle – la directive NIS 2 prévoit que les entités qui seront régulées par ses dispositions devront fournir aux autorités désignées par les États membres un certain nombre d'informations

La directive NIS 1 et **le dispositif SAIV** prévoyaient qu'il revenait à l'administration, et en l'occurrence en France à l'Agence nationale de sécurité des systèmes d'information (Anssi), de **désigner les entités** auxquelles s'appliquaient **les obligations en matière de cybersécurité prévues par NIS 1**.

Ces obligations concernaient en l'occurrence pour la France **environ 500 entités régulées**.

Avec la directive NIS 2 et le présent projet de loi de transposition, ce sont quelque **15 000 entités qui seront désormais régulées en France** en tant qu'entités « essentielles » ou « importantes », telles que définies aux articles 8 à 10 du projet de loi.

Le paragraphe 3 de l'article 3 de la directive NIS 2 prévoit qu'au plus tard le 17 avril 2025, **les États membres établissent une liste des entités « essentielles » et « importantes »** ainsi que **des entités fournissant des services d'enregistrement de noms de domaine**.

Les États membres **réexaminent cette liste** et, le cas échéant, **la mettent à jour régulièrement** et **au moins tous les deux ans** par la suite.

Le paragraphe 4 de l'article 3 prévoit également que les États membres **exigent des entités visées qu'elles communiquent aux autorités compétentes au moins les informations suivantes** :

- **le nom** de l'entité;

- **l'adresse** et **les coordonnées actualisées**, y compris **les adresses électroniques**, **les plages d'IP** et **les numéros de téléphone** ;
- le cas échéant, **le secteur et le sous-secteur concernés** visés à l'annexe I ou II ;
- le cas échéant, **une liste des États membres** dans lesquels **elles fournissent des services relevant du champ d'application de la directive**.

Les entités doivent **notifier sans tarder toute modification** des informations qu'elles ont communiquées et, en tout état de cause, **dans un délai de deux semaines à compter de la date de la modification**.

Le nombre d'entités visées étant désormais **très important**, le dernier alinéa du paragraphe 4 de l'article 3 de la directive NIS 2 dispose que les États membres peuvent **mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes**.

II. Le dispositif envisagé – la création d'un mécanisme d'auto-enregistrement obligatoire des entités régulées auprès de l'autorité nationale de sécurité des systèmes d'information

L'article 12 du présent projet de loi dispose que **l'autorité nationale de sécurité des systèmes d'information établit** et **met à jour la liste** des entités « essentielles », des entités « importantes » et des bureaux d'enregistrement **sur la base des informations** que ces entités et bureaux d'enregistrement **lui communiquent**.

En d'autres termes, il revient désormais à ces entités **d'évaluer elles-mêmes si elles entrent ou pas dans les critères définis par le projet de loi**, ce qui constitue **un transfert de responsabilité significatif**.

Ce renversement de la charge de l'identification s'appuie sur le dernier alinéa du paragraphe 4 de l'article 3 de la directive NIS 2 qui dispose que les États membres peuvent mettre en place **des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes**.

Si elles estiment **entrer dans ces critères**, alors elles **devront s'enregistrer auprès de l'autorité nationale de sécurité des systèmes d'information**, c'est-à-dire en l'occurrence de l'Autorité nationale de sécurité des systèmes d'information (Anssi) et lui communiquer **leur identité** et **toutes les informations** qui permettent d'expliquer en quoi **elles peuvent être considérées comme des entités relevant du projet de loi**.

Le deuxième alinéa de l'article 12 renvoie à un décret en Conseil d'État **la définition des informations à transmettre**, **leurs modalités de communication** et **les délais dans lesquels les modifications doivent être transmises par les entités concernées à l'ANSSI**.

Ce décret d'application devra transposer le paragraphe 4 de l'article 3 qui prévoit que les États membres exigent des entités visées qu'elles communiquent aux autorités compétentes **au moins les informations suivantes** :

- **le nom** de l'entité ;

- **l'adresse** et **les coordonnées actualisées**, y compris **les adresses électroniques**, **les plages d'IP** et **les numéros de téléphone** ;

- le cas échéant**, le secteur et le sous-secteur concernés** visés à l'annexe I ou II, ces secteurs et sous-secteurs étant visés à l'article 7 du présent projet de loi ;

- le cas échéant, **une liste des États membres dans lesquels elles fournissent des services** relevant du champ d'application de la directive.

Les entités devront **notifier sans tarder toute modification** des informations qu'elles ont communiquées et, en tout état de cause, **dans un délai de deux semaines à compter de la date de la modification**.

L'Anssi a d'ores-et-déjà créé **une plateforme en ligne baptisée MonEspaceNIS2** qui permet de **tester si une entité entre dans le champ d'application du projet de loi**.

Une fois ce dernier définitivement adopté et promulgué, cette plateforme **MonEspaceNIS2 devrait être utilisée pour procéder à l'enregistrement effectif des entités**.

III. La position de la commission – l'enregistrement par les entités elles-mêmes apparaît inévitable, eu égard à l'augmentation considérable d'entités régulées au titre de la cybersécurité

Le présent article 12 constitue **une transposition** des paragraphes 3 et 4 de l'article 3 de la directive NIS 2 qui fait le choix **d'activer la possibilité de mettre en place un mécanisme national permettant aux entités de s'enregistrer elle-même**.

Eu égard au nombre d'entités concernées par le titre II du projet de loi, évalué à **15 000**, **la mise en place d'un tel mécanisme au niveau français paraît effectivement incontournable**.

Votre rapporteur a pu **tester la plateforme en ligne baptisée MonEspaceNIS2**, laquelle propose déjà aux entités **une indication assez précise** de la probabilité qu'elles entrent dans le champ des entités régulées ou non par le présent projet de loi transposant la directive NIS 2.

Si la commission spéciale considère que le projet de loi renvoie trop souvent aux décret d'application, dans le cas de cet article, le renvoi à un décret d'application paraît fondé pour établir dans le détail **les informations à transmettre**, **leurs modalités de communication** et **les délais dans lesquels**

les modifications doivent être transmises, même si ces points sont **déjà partiellement prescrits dans la directive**, notamment **le délai des modifications** qui doivent être notifiées sans tarder et, en tout état de cause, **dans un délai de deux semaines** à compter de la date de la modification.

La commission n'a donc pas substantiellement modifié cet article, adoptant uniquement **un amendement COM 101 du rapporteur Patrick Chaize visant à insister sur la nécessité de mettre à jour au minimum tous les deux ans la liste des entités** visées par le titre II du présent projet de loi.

Elle a également adopté un amendement COM 20 du groupe Socialiste, Écologiste et Républicain prévoyant que **la CNIL est saisie pour avis sur le projet de décret en Conseil d'État** définissant les informations à transmettre au titre du présent article 12, dans la mesure où certaines d'entre elles peuvent avoir **un caractère personnel**.

La commission a adopté l'article ainsi modifié.

Article 13

Absence d'application des dispositions du projet de loi aux entités soumises à des exigences équivalentes en application d'un acte juridique de l'Union européenne

Cet article vise à prévoir les conditions dans lesquelles les dispositions du présent projet de loi peuvent ne pas s'appliquer aux entités soumises à des exigences équivalentes en application d'un acte juridique de l'Union européenne

La commission a adopté cet article sans modification.

I. La situation actuelle – la directive NIS 2 prévoit que ses dispositions peuvent ne pas s'appliquer aux entités soumises à des exigences équivalentes en application d'un acte juridique de l'Union européenne

L'article 4 de la directive NIS 2 porte sur **la combinaison entre les dispositions de la directive** et **d'autres actes juridiques sectoriels de l'Union européenne**.

Son paragraphe 1 prévoit ainsi que lorsque **des actes juridiques sectoriels** de l'Union imposent à des entités « essentielles » ou « importantes » d'adopter **des mesures de gestion des risques en matière de cybersécurité** ou **de notifier des incidents importants**, et lorsque ces exigences ont **un effet au moins équivalent à celui des obligations prévues par la directive**, **les dispositions pertinentes de la directive NIS 2**, y compris celles relatives à la supervision et à l'exécution prévues au chapitre VII, **ne sont pas applicables auxdites entités**.

Ce principe de *lex specialis* est notamment prévue pour permettre **la conciliation** entre **les dispositions de la directive NIS 2** d'une part, et celles **du règlement DORA** et de **la directive accompagnant ce règlement**, textes destinés à **améliorer la résilience du système bancaire et financier**.

Elle devrait s'appliquer également à certains types d'entité relevant des secteurs « Infrastructures numériques », « Gestion des services TIC » et « Fournisseurs numériques » tels que définis par les annexes de la directive NIS 2 car ces entités devraient faire l'objet **d'un règlement d'exécution spécifique de la Commission européenne**. Elles seront donc, dans ce cas particulier, soumises à **des mesures de gestion des risques cyber** et à **des obligations en matière de réponse à incident spécifiques**. Elles ne seront par conséquent **pas soumises aux mesures de sécurité ni aux règles de notification d'incidents s'appliquant aux entités régulées par NIS 2**.

En revanche, **lorsque des actes juridiques sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur spécifique** relevant du champ

d'application de la directive, **les dispositions pertinentes de la directive continuent de s'appliquer aux entités non couvertes par ces actes juridiques sectoriels de l'Union**.

Le paragraphe 2 de l'article 4 prévoit que les exigences visées au paragraphe 1 sont considérées comme ayant **un effet équivalent aux obligations prévues par la directive** lorsque :

- comme prévu en son point a), **les mesures de gestion des risques en matière de cybersécurité** ont **un effet au moins équivalent** à celui des mesures prévues à l'article 21 relatif **aux mesures de gestion des risques en matière de cybersécurité** ;
- comme prévu en son point b), l'acte juridique sectoriel de l'Union prévoit **un accès immédiat**, s'il y a lieu, **automatique et direct**, **aux notifications d'incidents par les *computer security incident response team* (CSIRT)**, les autorités compétentes ou les points de contact uniques en vertu de la directive.

II. Le dispositif envisagé – une transposition fidèle quoique incomplète de dispositions de la directive NIS 2 portant sur sa conciliation avec des actes juridiques de l'Union portant sur des exigences sectorielles en matière de cybersécurité

La première phrase de l'article 13 prévoit que **les dispositions pertinentes du présent projet de loi**, y compris **celles relatives à la supervision**, **ne sont pas applicables aux entités « essentielles » et « importantes » qui sont soumises**, en application **d'un acte juridique de l'Union européenne**, à **des exigences sectorielles de sécurité** et **de notification d'incidents** ayant **un effet au moins équivalent** aux obligations résultant des articles 14 et 17.

Cette transposition est fidèle au paragraphe 1 de l'article 4 de la directive, mais **ne reprend pas la précision** qui prévoit que **lorsque des actes juridiques sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur spécifique relevant du champ d'application de la directive**, les dispositions pertinentes de la directive **continuent de s'appliquer aux entités non couvertes par ces actes juridiques sectoriels de l'Union**.

Le renvoi à l'article 14, qui assure la transposition de l'article 21 relatif **aux mesures de gestion des risques en matière de cybersécurité**, permet de respecter la référence faite au même article 21 de la directive au point a) du paragraphe 2 de l'article 4 de la même directive.

La deuxième phrase de l'article 13 prévoit que pour être équivalentes, **les exigences de notification des incidents** doivent également prévoir **un accès immédiat aux notifications d'incidents** par l'autorité nationale de sécurité des systèmes d'information (c'est-à-dire l'Anssi).

Cette disposition est conforme au point b) du paragraphe 2 de l'article 4 de la directive qui dispose que l'acte juridique sectoriel de l'Union doit prévoir **un accès immédiat**, s'il y a lieu, **automatique et direct**, **aux notifications d'incidents** par les *computer security incident response team* (CSIRT), les autorités compétentes ou les points de contact uniques en vertu de la directive, cette responsabilité étant confiée à l'Anssi par l'article 17 du présent projet de loi.

III. La position de la commission – une transposition permettant une bonne conciliation entre dispositif général en matière de cybersécurité et réglementation sectorielle, mais la nécessité de prévoir un amendement pour éviter que des entités échappent à toute régulation

L'article 13 apparaît comme **une transposition fidèle** de l'article 4 de la directive NIS 2 et assure en particulier **l'articulation entre les dispositions transposant NIS 2** d'une part et celles **du règlement sur la résilience opérationnelle numérique du secteur financier (dit DORA)** et celles **transposant la directive accompagnant ce règlement d'autre part**.

Ces dispositions sont **nécessaires** pour **éviter que des entités se voient appliquer sur les mêmes sujets deux réglementations différentes**.

La commission spéciale **approuve ces dispositions de transposition** et n'a par conséquent pas apporté de modification au présent article 13**.**

La commission a adopté cet article sans modification.

Article 14

Mise en place de mesures de cybersécurité par les entités « essentielles » et « importantes »

Cet article prévoit que les entités « essentielles » et « importantes » sont tenues de prendre les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'informations qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

La commission a adopté deux amendements tendant à :

- insister sur la nécessaire proportionnalité de ces mesures, de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences économiques et sociales ;

- renforcer le rôle des organes de direction des entités régulées en matière de cybersécurité, en prévoyant que les organes de direction approuvent et supervisent les mesures de pilotage de la sécurité des réseaux et systèmes d'information, leurs membres ainsi que les personnes exposées aux risques devant être formés à la cybersécurité.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle – l'article 21 de la directive NIS 2 prévoit que les entités « essentielles » et « importantes » doivent prendre des mesures techniques, opérationnelles et organisationnelles pour gérer les risques cyber

Le paragraphe 1 de l'article 21 de la directive NIS 2 prévoit que les États membres veillent à ce que les entités « essentielles » et « importantes » prennent **les mesures techniques**, **opérationnelles** et **organisationnelles appropriées** et **proportionnées** pour **gérer les risques qui menacent la sécurité des réseaux** et **des systèmes d'information** que ces entités utilisent dans le cadre de **leurs activités** ou de **la fourniture de leurs services**, ainsi que **pour éliminer ou réduire les conséquences** que **les incidents** ont sur **les destinataires de leurs services** et sur **d'autres services**.

Les mesures visées doivent **garantir**, pour les réseaux et les systèmes d'information, **un niveau de sécurité adapté au risque existant**, en tenant compte de **l'état des connaissances** et, s'il y a lieu, **des normes européennes et internationales applicables**, ainsi que **du coût de mise en œuvre**.

Lors de l'évaluation de **la proportionnalité de ces mesures**, il convient de tenir dûment compte **du degré d'exposition de l'entité aux risques**, **de la taille de l'entité** et **de la probabilité de survenance d'incidents** et **de leur gravité**, y compris **leurs conséquences sociétales et économiques**.

Le paragraphe 2 de l'article 21 prévoit que ces mesures sont fondées sur **une approche « tous risques »** qui vise à **protéger les réseaux** et **les systèmes d'information** ainsi que **leur environnement physique contre les incidents**, et qu'elles comprennent au moins :

- les politiques relatives à **l'analyse des risques** et à **la sécurité des systèmes d'information** ;

- la gestion des incidents ;

- la continuité des activités, par exemple **la gestion des sauvegardes** et **la reprise des activités**, et **la gestion des crises** ;

- la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant **les relations entre chaque entité et ses fournisseurs ou prestataires de services directs** ;

- **la sécurité de l'acquisition**, **du développement** et **de la maintenance des réseaux et des systèmes d'information**, y compris **le traitement** et **la divulgation des vulnérabilités** ;

- des politiques et des procédures pour **évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité** ;

- les pratiques de base en matière de « **cyberhygiène** » et l**a formation à la cybersécurité** ;

- des politiques et des procédures relatives à **l'utilisation de la cryptographie** et, le cas échéant, **du chiffrement** ;

- la sécurité des ressources humaines, **des politiques de contrôle d'accès** et **la gestion des actifs** ;

- l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

II. Le dispositif envisagé – des obligations conformes aux dispositions de l'article 21 de la directive NIS 2 et qui feront l'objet d'un référentiel auquel devront se conformer les entités régulées

L'article 14 précise **les obligations** qui incombent aux différents acteurs assujettis aux dispositions du titre II du présent projet de loi transposant les dispositions de l'article 21 de la directive NIS 2.

Ces obligations s'appliquent :

- **aux entités « essentielles »** définies à l'article 8 ou susceptibles d'être désignées au titre de l'article 10 ;
- **aux entités « importantes »** définies à l'article 9 ou susceptibles d'être désignées au titre de l'article 10 ;
- **aux administrations de l'État** et **à leurs établissements publics administratifs** qui exercent leurs activités dans les domaines de **la sécurité publique**, de **la défense** et de **la sécurité nationale** ainsi que de **la répression pénale**, **les missions diplomatiques et consulaires française** pour leurs réseaux et systèmes d'information ;
- **au Commissariat à l'énergie atomique et aux énergies alternatives** pour ses activités dans le domaine de la défense ;
- **aux juridictions administratives et judiciaires**.

L'ensemble de ces acteurs sont tenus de **prendre les mesures techniques**, **opérationnelles et organisationnelles appropriées** et **proportionnées** pour :

- **gérer les risques qui menacent la sécurité des réseaux et des systèmes d'informations** qu'ils utilisent dans le cadre de **leurs activités** ou de **la fourniture de leurs services** ;
- **éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services** et **sur d'autres services**.

Il s'agit là précisément, retranscrites mot pour mot, **des obligations prévues par le premier paragraphe du 1 de l'article 21 de la directive NIS 2**.

Ces mesures techniques, **opérationnelles** et **organisationnelles** doivent garantir, **pour leurs réseaux** et **leurs systèmes d'information**, **un niveau de sécurité adapté** et **proportionné au risque existant**.

Si cette phrase figure au deuxième paragraphe du 1 de l'article 21 de NIS 2, la rédaction proposée ne précise pas, contrairement à la directive, qu'il s'agit de viser **un niveau de sécurité adapté et proportionné au risque existant** « *en tenant compte **de l'état des connaissances** et, s'il y a lieu, **des normes européennes et internationales applicables**, ainsi que **du coût de mise en œuvre*** ».

Il est également indiqué par la directive que « *lors de **l'évaluation de la proportionnalité de ces mesures**, il convient de tenir dûment compte **du degré d'exposition de l'entité aux risques**, **de la taille de l'entité** et **de la probabilité de survenance d'incidents** et **de leur gravité**, y compris **leurs conséquences sociétales et économiques*** ».

Il est bien précisé au dernier alinéa de l'article 14 que ces mesures sont mises en œuvre **aux frais des acteurs concernés**, ce qui représentera **pour ceux d'entre eux qui sont les moins matures des coûts importants**.

En vertu de l'article 14, ces mesures **techniques**, **opérationnelles** et **organisationnelles** visent à :

- Mettre en place **un pilotage de la sécurité des réseaux et systèmes d'information adapté**, comprenant notamment **la formation à la cybersécurité des membres des organes de direction** et **des personnes exposées aux risques**, problématique abordée, quoique de manière plus complète, par l'article 20 de la directive NIS 2 ;
- Assurer **la protection des réseaux** et **systèmes d'information**, y compris **en cas de recours à la sous-traitance** (il s'agit là d'une référence à la nécessité de prendre en compte « *la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs* » évoquée à l'article 21 de la directive) ;
- Mettre en place **des outils** et **des procédures** pour assurer **la défense des réseaux** et **systèmes d'information** et **gérer les incidents**, sujet lui aussi évoqué par l'article 21 de la directive ;
- **Garantir la résilience des activités**, point là aussi évoqué par l'article 21 de la directive.

L'article 14 prévoit qu'un décret en Conseil d'État :

- **Fixe les objectifs** auxquels doivent **se conformer les acteurs** auxquels s'applique le présent article, afin que les mesures adoptées pour la gestion des risques **satisfassent aux quatre obligations** énoncées ci-dessus ;
- Détermine **les conditions d'élaboration**, **de modification** et **de publication d'un référentiel d'exigences techniques et organisationnelles** qui sont **adaptées à ces différents acteurs**.

Il est précisé que ce référentiel peut **prescrire le recours à des produits**, **des services** ou **des processus certifiés** au titre du règlement (UE) n° 2019/881[1].

L'Anssi a indiqué à votre rapporteur que **les exigences de ce référentiel en matière de cybersécurité**, sur lequel elle travaille actuellement, s'inscriront **dans la suite logique de l'actuelle réglementation NIS 1** et porteront principalement sur **des aspects d'hygiène informatique fondamentale** afin que **les entités puissent se protéger contre les menaces les plus courantes**.

Selon le directeur de l'Anssi, il est envisagé que ce référentiel, dont votre rapporteur a pu consulter une version de travail, s'articule autour **d'une**

[1] *Règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013.*

vingtaine d'objectifs de sécurité obligatoires qui seront **la traduction technique**, **opérationnelle** et **organisationnelle** des mesures des articles 20 et 21 de la directive NIS 2.

Chaque objectif serait assorti **de mesures proposées** qui constitueraient des « ***moyens acceptables de mise en œuvre*** », dont le respect permettrait **d'atteindre les objectifs**. Mais ces mesures ne seraient **pas elles-mêmes obligatoires**, l'entité restant **libre de mettre en œuvre les moyens qu'elle souhaite** tant qu'ils permettent **l'atteinte des objectifs** susmentionnés qui, eux, seront **obligatoires**.

Selon l'Anssi, ces objectifs et mesures respecteront **un principe de proportionnalité** entre les entités « essentielles » et les entités « importantes » afin qu'il y ait **une différence claire** entre **les entités « essentielles »** qui devront respecter **un niveau d'exigence élevé**, et **les entités « importantes »**, qui constitueront **la majorité des nouveaux acteurs régulés**.

L'élaboration de ce référentiel est apparue comme **une nécessité**, **un renvoi à la norme ISO27001** n'étant **pas suffisant** (cf.**'encadré ci-après)**.

Il convient en outre de noter que, par défaut, **l'ensemble des systèmes d'information d'une entité seront concernées** par **le rehaussement des mesures de cybersécurité**, car ces systèmes sont **tous interdépendants** et susceptibles d'attaques cybercriminelles.

Celles-ci peuvent effectivement **viser des systèmes d'information annexes ou supports** et s'en servir pour se latéraliser vers le reste de l'infrastructure numérique.

Les entités « essentielles » et « importantes » conserveront néanmoins la possibilité **d'exclure du champ d'application certains de leurs systèmes** dont la défaillance n'aurait pas d'impact sur leur activité, selon des modalités qui seront précisées au niveau réglementaire.

Sont exclus du champ du décret en Conseil d'État mentionné *supra* et **autorisés à mettre en œuvre les exigences techniques et méthodologiques qui leur sont propres** les acteurs suivants :

- Les fournisseurs de services de systèmes de noms de domaine ;
- Les offices d'enregistrement ;
- Les fournisseurs de services d'informatique en nuage ;
- Les fournisseurs de services de centres de données ;
- Les fournisseurs de réseaux de diffusion de contenu ;
- Les fournisseurs de services gérés ;
- Les fournisseurs de sécurité gérés

- Les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux ;
- Les prestataires de services de confiance.

Place de la norme ISO27001 dans la transposition nationale de NIS 2

Pour transposer et mettre en œuvre la directive NIS 2, l'Anssi privilégie une approche de la conformité basée notamment sur la mise en œuvre du référentiel de mesures de cybersécurité adapté à la menace cybercriminelle mentionné à l'article 14. La norme ISO27001 et le référentiel de mesures cyber de l'ANSSI poursuivent en effet des objectifs différents. L'obtention d'une certification ISO27001 ne permet pas, en elle-même, une conformité à NIS 2. Mais cette norme constitue un outil et une méthodologie pour accompagner le déploiement du référentiel de sécurité.

L'ISO27001 établit des critères et propose une méthode pour la mise en place, la tenue à jour et l'amélioration continue d'un système de management de la sécurité de l'information (dit « SMSI ») sur un périmètre défini par l'entité. Un SMSI représente un ensemble de politiques et processus de protection des données basé sur le cadre règlementaire et une analyse de risques propre au périmètre de certification. L'ISO27001 ne prescrit pas de mesures cyber mais elle est complétée par la norme ISO27002 qui liste des « bonnes pratiques » pouvant être mises en œuvre. Il revient ainsi à l'entité de définir, elle-même, le niveau de sécurité à atteindre et le périmètre sur lequel il s'applique puis d'identifier et de mettre en œuvre les mesures de sécurité qu'elle juge nécessaires pour atteindre ce niveau de sécurité.

La directive NIS2 impose d'atteindre un niveau de sécurité nécessaire pour faire face à la menace cybercriminelle de masse. **Le référentiel élaboré par l'Anssi** définit les mesures de sécurité à mettre en œuvre, sur l'ensemble du système d'information (SI) de l'entité, pour atteindre cette cible de sécurité. Ce référentiel, en cohérence avec la directive intègre le principe de proportionnalité en adaptant le niveau de sécurité demandé en fonction de l'entité régulée (entité « essentielle » ou « importante »). À titre d'exemple, le référentiel de l'Anssi demande uniquement des sauvegardes pour les entités importantes (EI), là où il exige également des plans de continuité et de reprise d'activité pour les entités essentielles (EE). La norme ISO27001 n'impose quant à elle aucune exigence. La norme ISO27001, en tant que méthodologie, peut toutefois être utilisée comme méthode de mise en œuvre des mesures prescrites par le référentiel de mesures cyber de l'ANSSI.

Par ailleurs, **le référentiel Anssi** s'inscrit dans l'approche de simplification règlementaire portée par NIS 2. Il a été élaboré avec la

vocation de constituer **un socle commun** pour les régulations existantes et futures et ainsi limiter le « mille-feuille réglementaire ». Tout en préservant le cadre national et sa dépendance avec les enjeux de sécurité et de défense nationale, cette logique de « socle commun » permettra de favoriser la mise en place de mécanismes de **reconnaissance mutuelle** entre les référentiels NIS 2 des différents États membres au travers de travaux au sein du groupe de coopération NIS.

Enfin et dans cette même logique, il est à noter que **le volet résilience et en particulier la gestion de crise cyber**, axe majeur de la directive NIS 2 et de la transposition nationale, **n'est pas directement couvert par l'ISO27001** qui renvoie le sujet à l'ISO22301. La Belgique, face aux limites de la norme, a décidé de renforcer son référentiel NIS 2 national avec des exigences de résilience complémentaires à celles présentes dans l'ISO27001.

Source : Anssi

III. La position de la commission – des obligations en matière de sécurité indispensables, qui devront être décidées par les organes de direction des entités mais qui devront rester proportionnées et faire l'objet d'un accompagnement très soutenu

1) Élever le niveau de cybersécurité des entreprises et des administrations est une nécessité

Le présent article 14 permet d'assurer la transposition de l'article 21 de la directive NIS 2 en prévoyant que les entités « essentielles » et « importantes » devront **prendre les mesures techniques**, **opérationnelles et organisationnelles appropriées** et **proportionnées** pour :

- **gérer les risques qui menacent la sécurité des réseaux et des systèmes d'informations** qu'elles utilisent dans le cadre de **leurs activités** ou de **la fourniture de leurs services** ;
- **éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services** et **sur d'autres services**.

Il s'agit là d'une **des dispositions clefs du projet de loi**, à laquelle **la commission spéciale souscrit pleinement** : l'ensemble des entités visées par la transposition de la directive NIS 2 peuvent être **la cible de cyberattaques potentiellement dévastatrices** et doivent par conséquent **rehausser parfois fortement leur niveau de cybersécurité** pour y faire face.

2) Un impératif de proportionnalité pour éviter des obligations excessives et trop coûteuses

Cet impératif étant posé, il convient de **veiller à ce que les obligations** qui seront imposées à ces entités, et notamment **aux nombreuses**

entités « importantes », parfois de petite taille, demeurent **raisonnables** et **proportionnées**.

C'est la raison pour laquelle la commission spéciale a adopté un amendement COM 103 du rapporteur Patrick Chaize, directement inspiré par les dispositions de l'article 21 de la directive, qui prévoit que **les mesures adoptées par les entités** doivent permettre de viser **un niveau de sécurité adapté et proportionné au risque existant** « *en tenant compte* ***de l'état des connaissances*** *et, s'il y a lieu,* ***des normes européennes et internationales applicables****, ainsi que* ***du coût de mise en œuvre*** ».

Cet amendement vise également à inscrire dans la loi que « *lors de* ***l'évaluation de la proportionnalité de ces mesures****, il convient de tenir dûment compte* ***du degré d'exposition de l'entité aux risques****,* ***de la taille de l'entité*** *et* ***de la probabilité de survenance d'incidents*** *et* ***de leur gravité****, y compris* ***leurs conséquences sociétales et économiques*** ».

De fait, **les coûts** de mise en œuvre de ces mesures seront **très importants**, puisque l'Anssi les évalue à :

- **de 450 000 à 880 000 euros de coûts d'investissements** par entité, avec **un coût annuel de maintien en condition de sécurité** s'élevant à environ **10 % du coût d'investissement**, pour les entités « essentielles » ;
- **de 100 000 et 200 000 euros de coûts d'investissements** par entité, avec **un coût annuel de maintien en condition de sécurité** s'élevant à environ **10 % du coût d'investissement** pour les entités « importantes ».

Il s'agit là de **montant très significatifs**, d'où l'importance que les mesures qui seront prescrites, après concertation, par le référentiel de l'Anssi soient véritablement **conçues au plus près des réalités de terrain**, afin **d'éviter au maximum des exigences disproportionnées** qui ne seraient **pas adaptées aux entités concernées**, et notamment **les plus petites d'entre elles**.

En clair, il ne faudra **pas imposer des mesures draconiennes et coûteuses à une petite entreprise peu exposée à la menace cyber** ou pour laquelle **une attaque cyber aurait peu d'impact**.

3) <u>Insister davantage sur l'implication des organes de direction des entreprises</u>

Dans la rédaction initiale du projet de loi, il était prévu que les mesures que doivent prendre les entités régulées visent notamment à « *mettre en place un pilotage de la sécurité des réseaux et systèmes d'information adaptée, comprenant notamment* ***la formation à la cybersécurité des membres des organes de direction*** *et des personnes exposées aux risques* ».

Cette rédaction est apparue à la commission spéciale comme **une forme de sous-transposition de l'article 20 de la directive NIS 2** qui prévoit que **les décisions stratégiques en matière de cybersécurité** doivent être prises

par **les organes de direction des entreprises** ou **des administrations publiques** et que **leurs dirigeants** comme **leurs personnels exposés aux risques cyber** doivent être **formés aux grands enjeux en matière de cybersécurité**.

C'est pourquoi la commission spéciale à adopté **un amendement** COM 102 du rapporteur Patrick Chaize réécrivant le deuxième alinéa de l'article 14 pour prévoir que les mesures que prennent les entités régulées visent notamment à « *prévoir que* ***les organes de direction approuvent et supervisent les mesures de pilotage de la sécurité des réseaux et systèmes d'information****, leurs membres ainsi que les personnes exposées aux risques devant* ***être formés à la cybersécurité*** ».

Il paraît en effet indispensable, et conforme à l'esprit de la directive, d'insister sur le fait que **les organes de direction doivent approuver et superviser directement les mesures relatives à la cybersécurité**, ces questions essentielles relevant directement de **leur compétence** et de **leur responsabilité**.

4) Le rôle d'accompagnement de l'Anssi sera crucial pour réussir le rehaussement effectif de la cybersécurité des 15 000 entités qui devront appliquer les dispositions de ce projet de loi transposant la directive NIS 2

Le présent article 14 imposera à **15 000 entités** de s'engager dans **une démarche de rehaussement du niveau de sécurité de leurs systèmes d'information**, ce qui suscite **beaucoup d'inquiétudes** et de **demandes d'accompagnement**, ce qu'ont clairement montré les auditions réalisées par la commission spéciale.

Il sera donc crucial que **l'Anssi se mobilise très fortement** pour **faire connaître et comprendre les nouvelles obligations** prévues par la réglementation et assurer **leur mise en œuvre effective**.

Lors de son audition, le directeur général de l'Anssi a expliqué à la commission spéciale que **la plateforme en ligne MonEspaceNIS2** permettra **d'automatiser l'accompagnement des entités régulées** en devenant le vecteur de nombreuses informations, **la plateforme MonAideCyber** ayant pour sa part vocation à réaliser **des diagnostics de maturité de cybersécurité** et **d'identifier les mesures prioritaires** que l'entité devra appliquer **en termes de sécurité des systèmes d'information**.

Mais l'Anssi prévoit également de **s'appuyer fortement sur différents relais** tels que **les ministères coordonnateurs** (chargés de l'animation des communautés sectorielles), les organisations professionnelles, les associations de collectivités territoriales, l'écosystème de prestataires de services de cybersécurité ou bien encore le réseau de Campus Cyber national et régionaux en cours de déploiement.

De fait, la commission spéciale, si elle n'a pas vocation à légiférer sur ce point, ne saurait trop insister sur **la nécessité de prévoir un accompagnement très soutenu de l'ensemble des acteurs régulés** afin que ceux-ci puissent progressivement **se conformer à leurs obligations issues de la directive NIS 2**, sachant que le délai communément admis pour cette mise aux normes sera de **trois ans après la promulgation de la loi**.

La commission a adopté cet article ainsi modifié.

Article 15

Opposabilité à l'ANSSI en cas de contrôle de la mise en œuvre du référentiel qu'elle prescrit en matière de gestion des risques cyber

Cet article vise à rendre opposable à l'Anssi, en cas de contrôle effectué par elle, la mise en œuvre du référentiel qu'elle prescrit en matière de gestion des risques cyber.

La commission a adopté un amendement visant à créer un mécanisme de reconnaissance mutuelle entre les États membres de l'Union européenne, de sorte qu'une entité qui aurait vue certifiée sa conformité à la directive NIS 2 dans un autre État membre puisse s'en prévaloir lors d'un contrôle de l'Anssi, dès lors que celle-ci a validé le niveau équivalent de sécurité garanti par le référentiel dudit État membre.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle – une modalité directement introduite par la France pour simplifier la mise en œuvre des contrôles en matière de cybersécurité

Le présent article 15 **prend sens dans le contexte de la transposition de la directive NIS 2** mais ne trouve **pas son origine directement** dans l'une de ses dispositions.

Il constitue **une modalité d'application** faisant partie **de la marge de choix de l'État membre**.

II. Le dispositif envisagé – la création d'un dispositif d'opposabilité à l'Anssi en cas de contrôle de la mise en œuvre du référentiel qu'elle prescrit en matière de gestion des risques cyber

L'article 14 prévoit qu'un décret en Conseil d'État détermine les conditions d'élaboration, de modification et de publication **d'un référentiel d'exigences techniques et organisationnelles** adapté aux différents acteurs tenus d'atteindre les objectifs fixés par le même décret pour que **les mesures techniques, opérationnelles et organisationnelles** adoptées pour **la gestion des risques** permettent effectivement de :

- mettre en place **un pilotage de la sécurité des réseaux et systèmes d'information adapté**, comprenant notamment **la formation à la cybersécurité** des membres des organes de direction et des personnes exposées aux risques ;
- **assurer la protection des réseaux et systèmes d'information**, y compris en cas de recours à la sous-traitance ;
- mettre en place **des outils** et **des procédures** pour **assurer la défense des réseaux** et **systèmes d'information** et **gérer les incidents** ;

- Garantir **la résilience des activités**.

Il est précisé que ce référentiel peut prescrire le recours à des produits, des services ou des processus certifiés au titre du règlement (UE) n° 2019/881[1].

Le présent article 15 dispose que les acteurs qui **mettent en œuvre les exigences de ce référentiel** peuvent **s'en prévaloir auprès de l'Anssi lors d'un contrôle** pour **démontrer le respect des objectifs** qui leur sont fixés par le décret en Conseil d'État **en matière de gestion des risques cyber**.

Si ces acteurs ne mettent pas en œuvre les exigences de ce référentiel, ils seront **tenus de démontrer que les mesures qu'ils mettent en œuvre permettent de se conformer à ces objectifs en matière de gestion des risques cyber**.

Ainsi, l'utilisation du référentiel n'est **pas obligatoire** mais **très fortement incitée** dans la mesure où son application permet, lors d'un contrôle de l'Anssi, de **prouver efficacement** et **rapidement** que l'acteur contrôlé **s'est conformé à ses obligations** pour **atteindre ses objectifs en matière de gestion des risques cyber**.

Dans un souci **d'adaptation** et de **proportionnalité**, **le non recours au référentiel reste possible**, mais fait peser sur l'acteur **la charge de prouver qu'il a mis en œuvre des mesures techniques**, **opérationnelles** et **organisationnelles** qui lui permettent de **se conformer à ses objectifs** même si celles-ci ne correspondent pas, en tout ou partie, à celles qui sont prescrites par le référentiel.

III. La position de la commission – une mesure de simplification bienvenue, auquel il convient d'adjoindre un mécanisme de reconnaissance mutuelle des référentiels de niveau équivalent entre les États membres de l'Union européenne

Le présent article 15 ne vise pas à transposer une disposition de la directive, mais à mettre en place **un système d'opposabilité** pour **simplifier les contrôles de l'autorité nationale de sécurité des systèmes d'information** (c'est-à-dire de l'Anssi), ce qui a pour objet de faciliter la tâche de cette dernière mais également de protéger les entités qui se seront conformées aux exigences du référentiel prévu à l'article 14.

Les obligations mises à la charge des entités auxquelles s'appliquera le titre II du présent projet de loi étant très lourdes, la commission s'est montrée **très favorable** aux dispositions de cet article 15 qui introduisent **une mesure de simplification** et **d'efficacité bienvenue**, mais également **une**

[1] *Règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013.*

mesure de flexibilité en ne rendant pas le référentiel de l'Anssi **obligatoire**, même si **les entités régulées auront tout intérêt à s'y conformer**.

Afin de prévoir le cas **des entreprises exerçant leurs activités dans plusieurs États membres** et **appliquant partout un même référentiel qui ne serait pas celui de la France** mais qui serait **reconnu par l'Anssi elle-même comme de même niveau que son propre référentiel**, la commission spéciale a adopté un amendement COM 104 du rapporteur Patrick Chaize visant à créer **un mécanisme de reconnaissance mutuelle entre les États membres de l'Union européenne**, de sorte qu'une entité qui aurait vue certifiée sa conformité à la directive NIS 2 dans un autre État membre **puisse s'en prévaloir lors d'un contrôle de l'Anssi**, dès lors que celle-ci a **validé le niveau équivalent de sécurité garanti par le référentiel dudit État membre**.

La commission a adopté cet article ainsi modifié.

Article 16

Exigences de protection cyber supplémentaires pour les OIV et pour les administrations

Cet article vise à conférer au Premier ministre le pouvoir de rajouter des obligations supplémentaires en matière de cybersécurité aux opérateurs d'importance vitale (OIV) ainsi qu'aux administrations, en particulier les administrations régaliennes les plus sensibles

La commission a adopté cet article modifié par un amendement rédactionnel.

I. La situation actuelle – l'article 21 de la directive NIS 2 impose des obligations en matière de cybersécurité aux entités que celle-ci régule

Comme mentionné dans le commentaire de l'article 14, le paragraphe 1 de l'article 21 de la directive NIS 2 prévoit que les États membres veillent à ce que les entités « essentielles » et « importantes » prennent **les mesures techniques**, **opérationnelles** et **organisationnelles appropriées** et **proportionnées** pour **gérer les risques qui menacent la sécurité des réseaux** et **des systèmes d'information** que ces entités utilisent dans le cadre de **leurs activités** ou de **la fourniture de leurs services**, ainsi que **pour éliminer ou réduire les conséquences** que **les incidents** ont sur **les destinataires de leurs services** et sur **d'autres services**.

Le présent article 16 prévoit qu'à **ces obligations en matière de cybersécurité** s'en ajoutent d'autres pour **rehausser encore le niveau de sécurité des opérateurs d'importance vitale (OIV)** et **de plusieurs catégories d'administrations**.

II. Le dispositif envisagé – un dispositif de protection cyber renforcé par rapport aux autres entités régulées pour les OIV et pour les administrations de l'État auxquelles s'applique NIS 2.

L'article 1er du présent projet de loi prévoit, dans une disposition codifiée à l'article L. 1332-2 du code de la défense, que **sont désignés opérateurs d'importance vitale (OIV)** par l'autorité administrative :

- **Les opérateurs publics** ou **privés** exerçant, **au moyen d'infrastructures critiques** situées sur le territoire national, **une activité d'importance vitale**[1] ;

[1] *L'autorité administrative précise, le cas échéant, dans l'acte de désignation de l'opérateur d'importance vitale, l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur de l'Union européenne définis par le règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels et qui, à ce titre, doivent être regardés comme des entités critiques au sens de cette directive*

- **Les opérateurs publics** ou **privés**, gestionnaires, propriétaires ou exploitants **d'établissements mentionnés à l'article L. 511-1 du code de l'environnement** ou comprenant **une installation nucléaire de base** mentionnée à l'article L. 593-2 du même code, lorsque **la destruction** ou **l'avarie** d'une ou plusieurs installations de ces établissements peut présenter **un danger d'une particulière gravité pour la population ou l'environnement**.

Le premier alinéa de l'article 16 prévoit que **ces opérateurs d'importance vitale (OIV)** tiennent à jour et communiquent à l'autorité nationale de sécurité des systèmes d'information (c'est-à-dire l'Anssi) **la liste de leurs systèmes d'information d'importance vitale** selon les modalités fixées par le Premier ministre.

En vertu des dispositions du 2° de l'article L. 1332-1 du code de la défense tel qu'il résulte des dispositions de l'article 1er du présent projet de loi, **les systèmes d'information d'importance vitale des OIV** sont **les systèmes d'information nécessaires à l'exercice d'une activité d'importance vitale** ou **à la gestion**, **l'utilisation** ou **la protection d'une ou plusieurs infrastructures critiques**.

Les OIV devront donc **impérativement tenir à jour** et **communiquer à l'Anssi une liste de ces systèmes d'information d'importance vitale**.

Le deuxième alinéa de l'article 16 prévoit en outre que les OIV devront non seulement **mettre en œuvre sur leurs systèmes d'information d'importance vitale les exigences du référentiel mentionné à l'article 14** ainsi que **les exigences spécifiques à ces systèmes d'information fixées par le Premier ministre**. Pour ces OIV, se conformer au référentiel de l'Anssi ne suffira donc pas, il faudra également que **leurs systèmes d'information se conforment à des exigences spécifiques supplémentaires**.

Le troisième alinéa du présent article 16 prévoit que mettent en œuvre **les exigences du référentiel** mentionné à l'article 14 ainsi que **les exigences spécifiques** fixées par le Premier ministre à l'égard **des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations**, les entités suivantes :

- **les administrations** qui sont **entités « essentielles »** ou **« importantes »** ;
- **les administrations de l'État** et **leurs établissements publics administratifs** qui exercent leurs activités dans les domaines de **la sécurité publique**, de **la défense** et de **la sécurité nationale**, de **la répression pénale**, ou **des missions diplomatiques et consulaires françaises** et de leurs réseaux et systèmes d'information ;
- **le Commissariat à l'énergie atomique et aux énergies alternatives** pour ses activités dans le domaine de la défense ;
- **les juridictions administratives et judiciaires**.

Cela signifie que **pour chacune de ces administrations particulièrement sensibles** il sera nécessaire de **se conformer** non seulement **aux exigences du référentiel de l'Anssi** prévu par l'article 14 du présent projet de loi, mais également aux « ***exigences spécifiques*** *fixées par le Premier ministre à l'égard* ***des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations*** ».

Ces exigences devraient pour l'essentiel correspondre à celles du **référentiel général de sécurité (RGS)**[1] qui impose aux autorités administratives la mise en œuvre **de mesures de sécurité visant à limiter la fraude liée à l'usage des services numériques de ces administrations pour échanger avec leurs usagers ou d'autres administrations**.

Le quatrième alinéa de l'article 16 prévoit que les exigences spécifiques fixées par le Premier ministre prévues aux deuxièmes et troisième alinéas peuvent **prescrire le recours à des dispositifs matériels ou logiciels** ou à **des prestataires de services certifiés**, **qualifiés ou agréés** ou **prévoir que le recours à des dispositifs matériels ou logiciels ou à des prestataires de services certifiés**, **qualifiés ou agréés emporte présomption de conformité à l'exigence de sécurité concernée**.

Ces exigences peuvent également prescrire **des audits de sécurité réguliers réalisés par des organismes indépendants**.

Il est précisé que les personnes mentionnées au présent article 16 **appliquent ces exigences à leurs frais**.

Ce pouvoir de prescription de matériels, logiciels ou prestataires de service ou **de prescription d'audits de sécurité** se justifie par **le caractère particulièrement sensible des OIV et des administrations** visées au troisième alinéa de l'article 16, ce qui justifie que le Premier ministre, sur la base des travaux de l'Anssi, puissent faire preuve **d'exigences renforcées vis-à-vis de ces entités**.

III. La position de la commission – l'ajout d'exigences de cyber protections spécifiques pour les OIV et les administrations de l'État est justifiée, eu égard à la sensibilité de leurs systèmes d'information

Alors que l'article 14 du projet de loi prévoit que les entités régulées par le titre II transposant la directive NIS 2 devront mettre en œuvre **les mesures techniques**, **opérationnelles** et **organisationnelles appropriées** et **proportionnées** pour **gérer les risques qui menacent la sécurité de leurs réseaux** et **de leurs systèmes d'information**, l'article 16 confère au Premier ministre le pouvoir de **rajouter des obligations supplémentaires** pour **les**

[1] *C'est l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives qui avait introduit ce référentiel général de sécurité (RGS).*

opérateurs d'importance vitale (OIV) ainsi que pour **les administrations**, et en particulier **les administrations régaliennes les plus sensibles**.

Si **le principe de proportionnalité** invite à ne pas imposer des protections trop lourdes et coûteuses à des entités qui feraient l'objet de peu de menaces cyber ou dont une éventuelle défaillance aurait des conséquences limitées, il conduit également à prévoir que **des mesures renforcées** puissent être prévues **pour les entités les plus critiques ou les plus essentielles au bon fonctionnement de l'économie et de la société**.

La commission spéciale a donc considéré que les dispositions du présent article 16 **étaient proportionnées à leur objectif** et a seulement adopté un amendement rédactionnel COM 105 du rapporteur Patrick Chaize.

La commission a adopté cet article ainsi modifié.

Article 17

Obligation de notification à l'Anssi par les entités régulées des incidents importants en matière de cybersécurité, notification aux destinataires des services et information du public

Cet article prévoit que les entités régulées au titre de la directive NIS 2 doivent notifier à l'Anssi sans retard injustifié les incidents importants qu'elles subissent en matière de cybersécurité ayant un impact sur la fourniture de leurs services. Elles doivent également, sous réserve de plusieurs secrets protégés par la loi, en informer les destinataires de leurs services, voire le public.

La commission a adopté un amendement tendant à :

- définir la notion d'incident « important » *qui déclenche une notification à l'autorité nationale de sécurité des systèmes d'information ;*

- prévoir que la notification aux destinataires des services touchés par un incident important ou une vulnérabilité critique devra être faite « sans retard injustifié » *comme le prévoit la directive, et non* « sans délai » *tel que l'envisage la rédaction initiale de l'article 17 ;*

- supprimer la notion d'incident « critique » *qui crée de la confusion en venant s'ajouter à celle d'incident* « important » *;*

- prévoir les quatre étapes liées à la notification d'un incident important à l'autorité nationale de sécurité des systèmes d'information : alerte précoce dans les 24 heures, notification dans les 72 heures rapport intermédiaire et rapport final ;

- prévoir que l'autorité nationale de sécurité des systèmes d'information fournit, sans retard injustifié et si possible dans les 24 heures suivant la réception de la première notification reçue, une réponse à l'entité émettrice de la notification.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle – alors que l'Anssi est déjà destinataire de nombreuses notifications d'incidents de cybersécurité, la directive NIS 2 renforce ce rôle de CERT national auprès des entités dont elle prévoit la régulation

1) L'Anssi joue déjà un rôle clef en matière de réponses aux incidents en matière de cybersécurité

Comme rappelé dans le commentaire de l'article 5, **l'Agence nationale de la sécurité des systèmes d'information (Anssi)**, rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN), est **l'autorité de sécurité des systèmes d'information en France**, même s'il

convient également de noter que **le ministre de la défense** dispose lui aussi **de compétences spécifiques en matière de cybersécurité**[1].

L'Anssi s'est dotée en son sein **d'un CERT-France** qui assure les fonctions de ***Computer Emergency Response Team*** **(CERT)** ou ***Computer Security Incident Response Team*** **(CSIRT)** gouvernemental et national pour la France[2].

À ce titre, le CERT-France de l'Anssi est notamment destinataire **de déclarations d'incidents des opérateurs de services essentiels (OSE)** conformément à la loi n° 2018-133 de transposition de la directive NIS 1, **des opérateurs d'importance vitale (OIV)** concernant **leurs systèmes d'information d'importance vitale** en vertu de l'article L. 1332-6-2 du code de la défense, des incidents d'origine informatique **des opérateurs de communications électroniques** en vertu de l'article D. 98-5 du code des postes et des communications électroniques (CPCE) ou encore **des éditeurs de logiciels** en vertu de l'article L. 2321-4-1 du code de la défense.

Le CERT-France apporte ainsi **son appui 24h/24 et 7 jours/7 aux opérateurs d'importance vitale (OIV)**, **aux opérateurs de services essentiels (OSE)** mais également **aux ministères**, **aux autorités**, et à **d'autres organismes publics administratifs** dans leurs réponses **aux incidents de cybersécurité**.

A ce titre, **le CERT-France** est notamment chargé de :

- **détecter les vulnérabilités critiques** des systèmes d'information des entités supervisées, notamment via des services **d'audits techniques** et **d'audits automatisés**;
- aider à la mise en place **de moyens de protection** contre **d'éventuels incidents cyber futurs** ;
- après leur notification, assurer **les réponses aux incidents**, **l'assistance**, **le soutien**, **la remédiation** et la rédaction et diffusion **des bulletins** et **alertes** relatifs à **des vulnérabilités** permettant de les corriger ;
- favoriser et animer **un réseau de confiance**, avec différentes entités pour permettre **la bonne circulation de l'information**, et notamment **les connaissances sur les incidents** et **sur les menaces**.

Afin de démultiplier son action, l'Anssi a en outre **soutenu la création de CSIRT régionaux**, **sectoriels et ministériels** qui contribuent eux aussi à **la notification d'incidents**, à **l'aide à la remédiation** ainsi qu'à **la connaissance de la menace**.

---

[1] *Les compétences du ministre de la défense en matière de cybersécurité sont prévues par la sous-section 4 de la section 2 du chapitre Ier du titre Ier du livre IV du code de la défense.*

[2] *Les deux notions de CERT et de CSIRT ont le même sens et sont utilisés indifféremment.*

Les CSIRT régionaux, sectoriels et ministériels

A l'occasion du plan de relance 2020-2022, l'Anssi a soutenu l'émergence de CSIRT territoriaux, ministériels et sectoriels.

Douze CSIRT régionaux ont ainsi été ouverts en métropole, ainsi que trois centres de ressources cyber ultramarins (Nouvelle-Calédonie, Réunion, Territoires français d'Amériques), étape préliminaire à l'ouverture prochaine de leur CSIRT.

En lien avec les politiques économiques des territoires, ces structures offrent un premier niveau d'accompagnement aux PME, ETI, collectivités territoriales et associations locales, en assurant les premiers gestes de réponse à incident, en orientant les victimes vers des prestataires et en les coordonnant si nécessaire.

Elles les accompagnent aussi dans le dépôt de plainte et les déclarations obligatoires (à la Cnil par exemple) ainsi qu'en matière d'alertes sur les vulnérabilités.

Elles conduisent également des missions de prévention vis-à-vis des acteurs sur leurs territoires.

Sept CSIRT sectoriels ont également été créés, notamment dédiés aux établissements de santé, à l'enseignement supérieur, au secteur maritime et aux entreprises de défense.

Dotés des mêmes capacités que les CSIRT territoriaux, ils se spécialisent dans l'analyse de la menace et des impacts sectoriels aujourd'hui cruciaux pour des organisations à la chaîne d'approvisionnement complexe.

10 CSIRT ministériels viennent compléter ce maillage. Ils agissent au profit des administrations centrales des ministères pour leurs systèmes d'information centraux et apportent, en complément du CERT-France, des services de détection, de réponse à incident et d'analyse de la menace.

Enfin, l'Anssi accompagne et contribue à l'InterCERT France, association loi 1901 constituée en novembre 2021, qui vise à renforcer les liens de coopération et à accompagner la montée en maturité des CSIRT français, publics comme privés.

Ces réseaux de CSIRT permettent d'accroître le nombre d'entités en France ayant accès à des capacités de prévention, de détection, de partage d'information et de réaction aux incidents.

Source : Anssi

2) Les dispositions prévues par la directive NIS 2 en matière de notification aux CERT nationaux par les entités régulées des incidents

importants en matière de cybersécurité, de notification aux destinataires des services et d'information du public

Le point a) du paragraphe 3 de l'article 11 de la directive NIS 2 donne **au CSIRT national** la tâche **de surveiller** et **d'analyser les cybermenaces**, **les vulnérabilités** et **les incidents** au niveau national et, sur demande, **d'apporter une assistance aux entités « essentielles » et « importantes »** concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information.

En matière de notification, le paragraphe 1 de l'article 23 de la directive prévoit que chaque État membre doit veiller à ce que les entités « essentielles » et « importantes » **notifient**, **sans retard injustifié**, **à son CSIRT**, **tout incident ayant un impact important sur leur fourniture de service**.

En outre, le paragraphe 2 de l'article 23 prévoit que le cas échéant, les États membres veillent à ce que les entités « essentielles » et « importantes » **communiquent, sans retard injustifié**, **aux destinataires de leurs services** qui sont **potentiellement affectés par une cybermenace importante** toutes **les mesures ou corrections** que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, **les entités informent également ces destinataires de la cybermenace importante elle-même**.

Le paragraphe 3 de l'article 23 définit la notion **d'« *incident important* »**. Un incident est considéré comme **important** :

- s'il a causé ou est susceptible de causer **une perturbation opérationnelle grave des services** ou **des pertes financières** pour l'entité concernée;
- s'il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant **des dommages matériels**, **corporels** ou **moraux considérables**.

Pour mémoire, le paragraphe 6 de l'article 6 de la directive définit un incident de la façon suivante : « *un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles* ».

La notion d'incident important a par ailleurs été précisée par **le règlement d'exécution (UE) 2024/2690 du 17 octobre 2024**.

Le paragraphe 4 de l'article 23 élabore **un mécanisme échelonné** pour **la notification des incidents importants au CSIRT** pour les entités « essentielles » et « importantes », lequel comprend :

- **une « *alerte précoce* »**, **sans retard injustifié** et en tout état de cause **dans les 24 heures** après avoir eu connaissance de l'incident important, qui le cas échéant indique si l'on suspecte que l'incident important a été causé par **des actes illicites ou malveillants** ou s'il pourrait y avoir **un impact transfrontière** ;

- **une « *notification d'incident* », sans retard injustifié** et en tout état de cause **dans un délai de 72 heures** après avoir eu connaissance de l'incident important, qui le cas échéant met à jour les informations fournies au titre de l'alerte précoce, et fournit **une évaluation initiale de l'incident important**, y compris de **sa gravité** et de **son impact**, et **les indicateurs de compromission** lorsqu'ils sont disponibles ;
- à la demande du CSIRT, **un « *rapport intermédiaire* »** sur les mises à jour pertinentes de la situation ;
- **un « *rapport final* »**, dans un délai d'un mois, sous réserve que l'incident soit traité ;
- dans le cas contraire, **un « *rapport d'avancement* »**, dans un délai d'un mois, devant être complété par un rapport final dans un délai d'un mois après le traitement de l'incident.

La directive NIS 2 prévoit également, aux paragraphes 1 et 2 de son article 23 que les entités **notifient le cas échéant**, et **sans retard injustifié**, **aux destinataires de leurs services les incidents importants** susceptibles de **nuire à la fourniture de ces services** et qu'elles communiquent avec ceux affectés par **une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace**.

Une cybermenace importante est « *une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée* ***comme susceptible d'avoir un impact grave sur les réseaux*** *et* ***les systèmes d'information d'une entité*** *ou* ***les utilisateurs des services de l'entité****, en causant* ***un dommage matériel, corporel*** *ou* ***moral considérable*** ».

Enfin, le paragraphe 7 de l'article 23 la directive NIS 2, prévoit, lorsque **la sensibilisation du public est nécessaire** pour prévenir un incident important ou pour faire face à un incident important en cours, ou lorsque la divulgation de l'incident important est par ailleurs dans l'intérêt public, que le CSIRT d'un État membre peut, après avoir consulté l'entité concernée, **informer le public de l'incident important** ou **exiger de l'entité qu'elle le fasse**.

II. Le dispositif envisagé – une transposition qui renvoie trop de paramètres clefs de la notification d'incidents au niveau réglementaire

1) Une obligation de notification des incidents « importants » sans retard injustifié

Chargé à titre principal de transposer les dispositions de l'article 23 de la directive NIS 2, l'article 17 du présent projet de loi prévoit que les personnes mentionnées à l'article 14 ont l'obligation de **notifier à l'autorité nationale de sécurité des systèmes d'information** (c'est-à-dire l'Anssi, et en

son sein le CERT-France) **« *sans retard injustifié* » tout incident ayant un impact « *important* » sur la fourniture de leurs services**.

En vertu de l'article 14, ces obligations s'appliquent :

- **Aux entités « essentielles »** définies à l'article 8 ou susceptibles d'être désignées au titre de l'article 10 ;

- **Aux entités « importantes »** définies à l'article 9 ou susceptibles d'être désignées au titre de l'article 10 ;

- **Aux administrations de l'État** et **à leurs établissements publics administratifs** qui exercent leurs activités dans **les domaines de la sécurité publique**, **de la défense** et **de la sécurité nationale** ainsi que **de la répression pénale**, **les missions diplomatiques et consulaires française** pour leurs réseaux et systèmes d'information ;

- **Au Commissariat à l'énergie atomique et aux énergies alternatives** pour ses activités dans le domaine de la défense ;

- **Aux juridictions administratives et judiciaires**.

Alors que le paragraphe 3 de l'article 23 de la directive NIS 2, définit **la notion d'« *incident important* »**, le premier alinéa de l'article 17 du présent projet de loi **ne le définit pas**.

Il convient également de noter qu'alors que le paragraphe 4 de l'article 23 de la directive définit **quatre étapes de notification au CSIRT national** en cas d'incident important – dans les 24 heures, dans les 72 heures, puis rapport intermédiaire et enfin rapport final – le premier alinéa de l'article 17 du présent projet de loi évoque uniquement une notification « *sans retard injustifié* », les modalités de cette notification et notamment ses délais **étant renvoyés au niveau réglementaire**.

2) Notification des incidents « importants » aux destinataires des services et au public

Pour **prévenir un incident** concernant une entité « essentielle » ou une entité « importante », ou pour **faire face à un incident en cours**, ou lorsque **la divulgation de l'incident est dans l'intérêt public**, le deuxième alinéa de l'article 17 autorise l'Anssi, après avoir consulté l'entité « essentielle » ou « importante » concernée, à **exiger d'elle qu'elle informe le public de l'incident**, ou **le faire elle-même**.

Il s'agit là **d'une transposition fidèle** du paragraphe 7 de l'article 23 de la directive NIS 2.

3) Obligation de notification des incidents « critiques » et des vulnérabilités « critiques » aux destinataires des services et au public

Le troisième alinéa de l'article 17 et les suivants prévoient que les entités « essentielles » et « importantes » **doivent notifier « sans délai » aux destinataires de leurs services** :

- **les « incidents critiques »** susceptibles de **nuire à la fourniture de ces services** ;
- **les « vulnérabilités critiques » affectant leurs services** ou **les affectant potentiellement**, ainsi que **les mesures ou corrections**, dès qu'elles en ont connaissance, que **ces destinataires peuvent appliquer en réponse à cette vulnérabilité ou à cette menace**.

La disposition relative **aux « *incidents critiques* »** paraît correspondre à la deuxième phrase du paragraphe 1 de l'article 23 de la directive qui dispose que *« le cas échéant, les entités concernées notifient, sans retard injustifié,* ***aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services*** ».

Le fait d'introduire la notion **d'« *incidents critiques* »** en lieu et place de la notion **d' « *incidents importants* »** prévue par la directive, et du reste reprise au premier alinéa du présent article 17, est toutefois **source de complexité** et **de confusion**.

La disposition relative aux « *vulnérabilités critiques* » paraît quant à elle correspondre au paragraphe 2 de l'article 23 de la directive qui dispose que « *les États membres veillent à ce que les entités essentielles et importantes* ***communiquent, sans retard injustifié, aux destinataires de leurs services*** *qui sont* ***potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace****. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même* ».

Là encore, l'introduction de **la notion de « *vulnérabilité critique* »** alors que la directive porte celle de « *cybermenace importante* » n'est pas pleinement satisfaisante, même si la notion de « cybermenace » ne paraît guère adaptée d'un point de vue légistique.

Enfin, le troisième alinéa de l'article 17 évoque une notification **« *sans délai* »** là où la directive prévoit une notification « ***sans retard injustifié*** ». Cette différence ne peut être, une nouvelle fois, que **source de difficultés**.

4) Protection des secrets et des données personnelles

Les dispositions de l'article 17 prévoient que cette obligation de notification des incidents critiques et des vulnérabilités critiques ne s'étend toutefois **pas aux informations dont la divulgation porterait atteinte aux intérêts de la défense et de la sécurité nationale**.

En cas d'incident critique ou de vulnérabilité critique, les personnes auxquelles s'appliquent les dispositions du présent article 17 peuvent **communiquer à l'Anssi la liste des destinataires de leurs services**.

L'Anssi tient compte, dans l'usage qu'elle fait de ces informations, **des intérêts économiques de ces personnes** et veille à **ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en matière commerciale et industrielle**.

En outre, l'ANSSI **doit informer la Commission nationale de l'informatique et des libertés (Cnil)** de tout incident susceptible d'entraîner **une violation de données à caractère personnel**.

Il est enfin prévu qu'un décret en Conseil d'État fixe les modalités d'application du présent article 17.

Ce décret précise notamment la procédure applicable et **les critères d'appréciation des caractères « *important* » et « *critiques* » des incidents et vulnérabilités** ainsi que les délais de notification des incidents et des vulnérabilités.

III. La position de la commission – de nombreuses modifications destinées à adopter une rédaction plus complète, plus claire et plus conforme aux dispositions de la directive NIS 2

Si la rédaction proposée pour l'article 17 assure globalement **une transposition correcte de l'article 23 de la directive NIS 2**, la commission spéciale a toutefois considéré que **de nombreuses dispositions clefs de cet article étaient renvoyées au niveau réglementaire** alors qu'il paraissait plus judicieux de **les faire figurer directement dans la loi** dans un souci de **clarté juridique**.

En outre, **plusieurs notions ou définitions** lui ont paru devoir être **précisées ou corrigées** pour **éviter toute confusion** et permettre **une meilleure sécurité juridique**.

1) Préciser la notion d'« *incident important* » pour éviter toute ambiguïté.

La notion **d'incident important** est essentielle pour la bonne application de l'article 17 car c'est lorsqu'un incident est qualifié d'« *important* » que l'entité régulée doit **le notifier à l'Anssi**.

Il est donc souhaitable d'inscrire dans la loi **la définition précise** d'ores-et-déjà prévue par le paragraphe 3 de l'article 23 qui dispose qu'**un incident est considéré comme important** :

- s'il a causé ou est susceptible de causer **une perturbation opérationnelle grave des services** ou **des pertes financières** pour l'entité concernée;

- s'il a affecté ou est susceptible **d'affecter d'autres personnes physiques ou morales** en causant **des dommages matériels**, **corporels** ou **moraux considérables**.

La commission spéciale a adopté en ce sens l'amendement COM 106 du rapporteur Patrick Chaize.

2) Introduire les délais prévus par la directive : 24 heures, 72 heures, rapport intermédiaire et rapport final

Comme rappelé *supra*, alors que le paragraphe 4 de l'article 23 de la directive définit **quatre étapes de notification au CSIRT national en cas d'incident important** – dans les 24 heures, dans les 72 heures, puis rapport intermédiaire et enfin rapport final – le premier alinéa de l'article 17 du présent projet de loi évoque uniquement **une notification « *sans retard injustifié* » à l'Anssi**.

Or ces délais inscrits dans la directive sont le fruit **d'un compromis longuement débattu** entre les colégislateurs européens lors de l'adoption de la directive.

S'il semble légitime de recourir à la voie réglementaire pour prévoir les modalités pratiques de cette obligation, **il est indispensable que le projet de loi respecte la lettre de la directive NIS 2 concernant ces délais**.

De fait, **d'éventuelles législations hétérogènes** entre États membres sur la procédure de notification **complexifieraient considérablement l'application du texte pour les entreprises** qui sont présentes dans plusieurs États.

La commission spéciale a par conséquent adopté l'amendement COM 106 du rapporteur Patrick Chaize qui prévoit que **les personnes mentionnées à l'article 14 soumettent à l'autorité nationale de sécurité des systèmes d'information (c'est-à-dire l'Anssi)** :

- **sans retard injustifié** et en tout état de cause **dans les vingt-quatre heures** après avoir eu connaissance de l'incident important, **une alerte précoce** qui, le cas échéant indique s'il est suspecté que l'incident important a été causé **par des actes illicites ou malveillants** ou s'il pourrait avoir **un impact hors du territoire national** ;

- **sans retard injustifié** et en tout état de cause **dans un délai de soixante-douze heures** après avoir eu connaissance de l'incident important, **une notification d'incident** qui, le cas échéant, **met à jour les informations fournies au titre de l'alerte précoce**, et fournit **une évaluation initiale de l'incident important**, y compris **de sa gravité et de son impact**, et **les indicateurs de compromission** lorsqu'ils sont disponibles ;

- à la demande de l'autorité nationale de sécurité des systèmes d'information, **un rapport intermédiaire sur l'évolution de la situation** ;

- **un rapport final** au plus tard un mois après la notification d'incident, sous réserve que l'incident soit traité ;

- dans le cas contraire, **un rapport d'avancement**, dans un délai d'un mois, devant être **complété par un rapport final** dans un délai d'un mois après le traitement de l'incident.

3) Prévoir une obligation de réponse de l'Anssi sans retard injustifié

Le paragraphe 5 de l'article 23 prévoit que **le CSIRT ou l'autorité compétente fournissent**, **sans retard injustifié** et **si possible dans les 24 heures suivant la réception de l'alerte précoce** visée au point a) du paragraphe 4, **une réponse à l'entité émettrice de la notification**, y compris **un retour d'information initial sur l'incident important** et, à la demande de l'entité, des orientations ou des conseils opérationnels **sur la mise en œuvre d'éventuelles mesures d'atténuation**.

Or **cette obligation n'a pas été reprise à l'article 17** assurant la transposition de l'article 23 de la directive.

Beaucoup d'obligations sont mises à la charge des entités régulées par le titre II du présent projet de loi, et en particulier **les entreprises** et **les collectivités territoriales**.

C'est pourquoi il est important, par parallélisme, **d'inscrire également dans la loi les obligations qui incombent à l'Anssi vis-à-vis des entités régulées**.

C'est pourquoi il est apparu souhaitable à la commission spéciale d'introduire à l'article 17 un alinéa indiquant que « ***l'autorité nationale de sécurité des systèmes d'information fournit, sans retard injustifié et si possible dans les 24 heures suivant la réception de la première notification reçue, une réponse à l'entité émettrice de la notification****, y compris un retour d'information initial sur l'incident important et, à la demande de l'entité, des orientations ou des conseils opérationnels* ***sur la mise en œuvre d'éventuelles mesures d'atténuation*** », ce qui a été fait par l'amendement COM 106 du rapporteur Patrick Chaize

4) Supprimer la notion d'incident « critiques », source de confusion

Toujours à l'article 17, la commission spéciale a **supprimé** grâce à l'amendement COM 106 du rapporteur Patrick Chaize **la notion d'incidents « *critiques* »**, pour se limiter à **la seule notion d'incidents « *importants* » prévue par la directive**.

Rajouter cette catégorie supplémentaire était **source de confusion** et **donc d'insécurité juridique**.

Enfin, au troisième alinéa, la commission spéciale a prévu que la notification aux destinataires des services touchés par un incident important ou une vulnérabilité critique devrait être **faite « *sans retard injustifié* » comme le prévoit la directive**, et **non « *sans délai* »** tel que l'envisageait la rédaction initiale de l'article 17, **cette différence pouvant**, là encore, **être potentiellement source de difficultés**.

La commission a adopté cet article ainsi modifié.

Article 18

Détermination des critères territoriaux pour l'application aux offices et aux bureaux d'enregistrement des noms de domaine

Cet article vise à définir par des critères territoriaux de compétence les offices d'enregistrement et les bureaux d'enregistrement auxquels s'appliquent les dispositions de la section 3 « Enregistrement des noms de domaine ».

La commission a adopté cet article sans modification.

I. La situation actuelle – la directive NIS 2 impose des obligations aux offices et aux bureaux d'enregistrement en matière et collecte et de mise à jour des données d'enregistrement des noms de domaine

La directive NIS 1 ne prévoyait pas, dans son champ d'application, d'obligations pour **les bureaux d'enregistrement**, ni de dispositions relatives à **la sécurisation des noms de domaines génériques**.

Au niveau national, **le seul cadre juridique existant relatif aux noms de domaine** est aujourd'hui celui prévu par aux articles L. 45 à L. 45-8 du code des postes et des communications électroniques (CPCE). Il porte uniquement sur **l'enregistrement et l'attribution des noms de domaine de premier niveau** (ex : « .fr », cf. explications dans l'encadré *infra*).

La directive NIS 2 opère un changement important en intégrant à son article 28 **les offices d'enregistrement** pour ce qui concerne **les obligations de sécurisation**, et **les bureaux d'enregistrement** pour ce qui relève de **la collecte et de la mise à jour des données d'enregistrement des noms de domaine**.

L'objectif de cet article 28 est de **permettre aux autorités chargées de la sécurité des systèmes d'information** ou **aux autorités judiciaires** de pouvoir **accéder**, **à leur demande** et dans **un délai maximal de 72 heures**, à **des données exactes** permettant **d'identifier le propriétaire d'un nom de domaine** en cas **d'incident de cybersécurité** et, dans le même temps, **d'harmoniser les règles au niveau européen**.

Dans cette perspective, l'article 28 prévoit que les États membres doivent **imposer aux offices d'enregistrement de collecter** et **de conserver certaines données d'enregistrement des noms de domaine** (nom du titulaire, point de contact, nom du domaine…) et **organiser l'accès à ces données aux autorités légitimes**, ainsi que **la publicité des procédures prévues à cet effet**.

L'article 28 de la directive prévoit également que les États membres doivent prendre des mesures pour **s'assurer de la fiabilité des serveurs** et **des bases de données des offices d'enregistrement des noms de domaine**.

Le système de nom de domaine, les offices d'enregistrement et les bureaux d'enregistrement

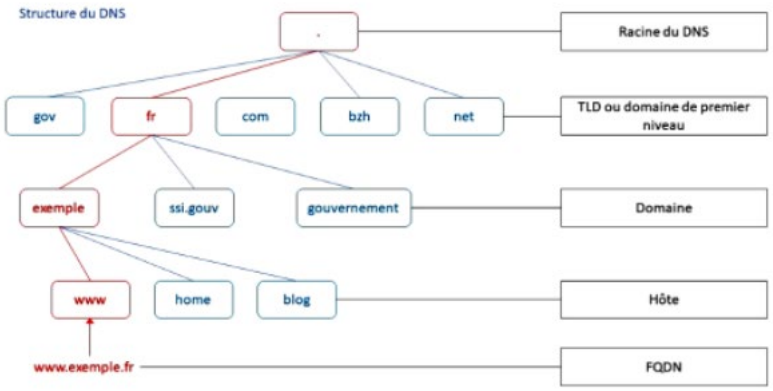
Le « Domain Name System » (système de nom de domaine) ou DNS est un service permettant de faire correspondre un nom de domaine à une adresse IP *(Internet Protocol*) – le numéro attribué à titre permanent ou provisoire à chaque périphérique relié à Internet, adresse qui prend la forme d'une suite de numéros (par exemple, « 45.60.12.53 ») et est compréhensible par une machine.

Le nom de domaine (URL ou *Uniform Resource Locators*, « localisateur uniforme de ressource », sous la forme « exemple.fr »), plus facile à retenir et à retranscrire pour l'internaute, constitue l'alias alphanumérique de l'adresse IP. Les machines appelées serveurs de nom de domaine (ou serveurs DNS) permettent d'établir la correspondance entre le nom d domaine et l'adresse IP des machines d'un réseau.

Le système DNS s'appuie sur une structure arborescente. L'ensemble des noms de domaine constituent ainsi un arbre inversé où chaque nœud est séparé du suivant par un point. On appelle « nom de domaine » chaque nœud de l'arbre. Le nom absolu, correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (*Fully Qualified Domain Name*). À titre d'exemple, « legifrance.gouv.fr. » constitue une adresse FQDN.

Lorsqu'une requête relative à un nom de domaine est effectuée, des serveurs sont successivement interrogés pour retrouver l'adresse IP correspondante. Si l'on cherche par exemple le nom de domaine « exemple.fr », dans un premier temps, un serveur racine est interrogé, qui renvoie vers le serveur faisant autorité pour le domaine de premier niveau, appelé le *Top Level Domain* ou extension (« .fr » dans l'exemple).

Dans un second temps, le serveur autorité de premier niveau renvoie l'adresse du serveur faisant autorité sur le second niveau (ici, « exemple.fr »), et cela jusqu'à ce que la requête soit résolue.



Le domaine de premier niveau est, dans le système de noms de domaine internet, un sous-domaine de la racine. Il est possible de les distinguer en trois principales catégories :

- domaine de premier niveau spécial (à des fins techniques, tel le « .arpa » relatif aux paramètres d'adressage et de routage) ;
- domaines de premier niveau nationaux (correspond à un pays ou un territoire de celui-ci. Ex : « .fr », « .nc ») ;
- domaines de premier niveau génériques (correspond en général à un secteur d'activité). Ces domaines se divisent en domaines génériques non parrainés (« .net », « .org » pour les organisations à but non lucratif, « .com » pour les organisations à but lucratif, « .pro » etc…) et en domaines génériques parrainés (« .gov » pour les organismes gouvernementaux américains).

Chaque domaine de premier niveau est géré par une organisation qui est chargée d'allouer (éventuellement de manière commerciale) ses sous-domaines, aussi appelée office d'enregistrement.

Cet office d'enregistrement est une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage.

À titre d'exemple, en application de l'article L. 45 du code des postes et des communications électronique, l'office d'enregistrement en charge du domaine de premier niveau du « .fr » est l'Association française pour le nommage Internet en coopération (AFNIC), qui agit sur délégation du ministre chargé des communications électroniques.

Dans cet environnement, les bureaux d'enregistrement, qui sont des entités fournissant des services d'enregistrement de noms de domaine, exercent leur activité d'intermédiaire auprès de l'office d'enregistrement d'une part et des professionnels et particuliers d'autre part. Ils sont accrédités par les offices d'enregistrement à cette fin. À titre d'illustration, l'AFNIC répertorie comme bureaux d'enregistrement Orange, SFR (pour les fournisseurs d'accès à internet), Gandi, OVH ou bien encore *Nameshield*.

Source : Étude d'impact du projet de loi

II. Le dispositif envisagé – critères territoriaux pour définir l'application de la présente section aux offices d'enregistrement et aux bureaux d'enregistrement des noms de domaine

La section 3 « *Enregistrement des noms de domaine* » du titre II du projet de loi, qui correspond aux articles 18 à 22 du projet de loi, est entièrement consacrée à **la transposition de l'article 28 de la directive NIS 2** concernant **l'enregistrement des noms de domaine**.

A noter que cette section 3 ne modifie pas les articles L. 45 à L. 45-8 du code des postes et des communications électroniques (CPCE), dont l'objet et le champ d'application sont différents de ceux visés par l'article 28 de la directive NIS 2.

L'article 18 prévoit que **les offices d'enregistrement de noms de domaine** et **les bureaux d'enregistrement de noms de domaine** ainsi que **les agents agissant pour le compte de ces derniers** qui satisfont à l'une des conditions prévues à l'article 11 sont **soumis aux dispositions de la présente section 3 « *Enregistrement des noms de domaine* »**.

1) Les offices d'enregistrement des noms de domaine et les critères d'application de la présente section 3

Pour mémoire, le 2° de l'article 6 du présent projet de loi définit un office d'enregistrement comme « *une entité à laquelle **un domaine de premier niveau spécifique a été délégué** et qui est **responsable de l'administration de ce domaine**, y compris de **l'enregistrement des noms de domaine** en relevant et de **son fonctionnement technique**, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution de ses fichiers de zone sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage* ».

Le 3° du I de l'article 11 dispose qu'il faut, pour que les dispositions de la présente loi s'appliquent aux offices d'enregistrement :

- qu'ils aient **leur établissement principal sur le territoire national** ;

- ou, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national, qu'ils aient désigné **un représentant établi sur le territoire national**.

2) Les bureaux d'enregistrement des noms de domaine et les critères d'application de la présente section 3

Pour mémoire, le deuxième alinéa de l'article 6 définit un bureau d'enregistrement comme « ***une entité fournissant des services d'enregistrement de noms de domaine*** ».

S'agissant des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers, les obligations du titre II concernent :

- ceux qui ont **leur établissement principal sur le territoire national** ;

- ou ceux qui ont désigné **un représentant établi sur le territoire national**, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national.

Le III de l'article 11 précise que **l'établissement principal** s'entend du lieu :

- où sont principalement prises **les décisions relatives aux mesures de gestion des risques en matière de cybersécurité** ;

- ou, à défaut, le lieu où **les opérations de cybersécurité** sont effectuées ;

- ou, à défaut, l'établissement comptant **le plus grand nombre de salariés dans l'Union européenne**.

S'agissant de la notion de représentant, celle-ci est définie au 5° de l'article 6 comme « ***une personne physique ou morale établie dans l'Union*** *qui est expressément désignée pour agir pour le compte d'un fournisseur de services de système de nom de domaine, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine* […] *qui peut être contacté par une autorité compétente ou un centre de veille, d'alerte et de réponse aux attaques informatiques (CERT) à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi* ».

III. La position de la commission – un article destiné à établir les critères territoriaux pour l'application des dispositions de la section 3 aux offices et aux bureaux d'enregistrement

Le présent article 18 établit, en faisant référence aux dispositions de l'article 11, **les critères territoriaux d'application aux offices d'enregistrement et aux bureaux d'enregistrement** des dispositions de la section 3 « Enregistrement des noms de domaine » qui vient transposer **les dispositions de l'article 28 de la directive NIS 2**.

Il constitue donc **une mesure de transposition nécessaire** et n'appelle pas de commentaires de la part de la commission spéciale.

La commission a adopté cet article sans modification.

Article 19

Obligation pour les offices et les bureaux d'enregistrement des noms de domaine de mettre en place une base de données

Cet article oblige les offices et les bureaux d'enregistrement des noms de domaine de mettre en place une base de données afin de pouvoir accéder aux données permettant d'identifier le propriétaire d'un nom de domaine en cas d'incident.

La commission a adopté cet article sans modification.

I. La situation actuelle – la directive NIS 2 prévoit que les Etats membres imposent aux offices et aux bureaux d'enregistrement la collecte et la conservation dans une base de données de certaines données d'enregistrement des noms de domaine

Afin **d'harmoniser les règles à l'échelle européenne** et **de pouvoir accéder aux données** permettant **d'identifier le propriétaire d'un nom de domaine en cas d'incident**, l'article 28 de la directive NIS 2 prévoit **de nouvelles règles en matière d'enregistrement des noms de domaine**.

En vertu de son paragraphe 1, les États membres doivent **imposer aux offices d'enregistrement** de **collecter certaines données d'enregistrement des noms de domaine** (nom du titulaire, point de contact, nom du domaine…) et de **les maintenir exactes et complètes** au sein **d'une base de données spécialisée** avec **la diligence requise par le droit de l'Union en matière de protection des données** pour ce qui concerne **les données à caractère personnel**.

À cette fin, le paragraphe 2 de l'article 28 prévoit que les États membres exigent que **la base des données d'enregistrement des noms de domaine** contienne **les informations nécessaires** pour **identifier** et **contacter les titulaires des noms de domaine** et **les points de contact** qui **gèrent les noms de domaine relevant des domaines de premier niveau**.

Ces informations comprennent notamment les éléments suivants :

- le nom de domaine ;

- la date d'enregistrement ;

- le nom du titulaire, l'adresse de courrier électronique et **le numéro de téléphone** permettant de le contacter ;

- l'adresse de courrier électronique et **le numéro de téléphone** permettant de contacter **le point de contact qui gère le nom de domaine**, si ces coordonnées sont différentes de celles du titulaire.

Le paragraphe 3 prévoit que les États membres exigent que **les registres des noms de domaine de premier niveau** et **les entités fournissant des services d'enregistrement de noms de domaine** aient mis en place **des**

politiques et **des procédures**, notamment **des procédures de vérification**, visant à garantir que **les bases de données contiennent des informations exactes et complètes**.

Les États membres imposent que **ces politiques et procédures** soient mises à **la disposition du public**.

En vertu du paragraphe 4, les États membres exigent que **les registres des noms de domaine de premier niveau** et **les entités fournissant des services d'enregistrement de noms de domaine** rendent **publiques**, sans retard injustifié après l'enregistrement d'un nom de domaine, **les données d'enregistrement du nom de domaine** qui ne sont **pas des données à caractère personnel**.

Le paragraphe 6 précise que le respect de ces obligations **ne saurait entraîner de répétition inutile de la collecte des données d'enregistrement de noms de domaine**.

À cet effet, les États membres imposent aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine **de coopérer entre eux**.

II. Le dispositif envisagé – une obligation de collecte de données puis de tenue d'une base de données par les offices et bureaux d'enregistrement

Le premier alinéa de l'article 19 prévoit que **les offices d'enregistrement collectent**, par l'intermédiaire **des bureaux d'enregistrement** ainsi que des agents agissant pour le compte de ces derniers, **les données nécessaires à l'enregistrement des noms de domaine**, transposant ainsi l'obligation prévue au paragraphe 1 de l'article 28.

Les offices et les bureaux d'enregistrement sont **responsables du traitement de ces données** au regard de **la réglementation en matière de protection des données personnelles**, ainsi que le prévoit le paragraphe 1 de la directive qui évoque la nécessité de faire preuve de « *la diligence requise par le droit de l'Union en matière* ***de protection des données*** *pour ce qui concerne* ***les données à caractère personnel*** ».

Les offices et les bureaux d'enregistrement ont l'obligation de **tenir ces bases de données à jour**, en maintenant **les données exactes et complètes**, **sans redondance de collecte**.

Le paragraphe 1 de l'article 28 évoque **cette obligation de collecte** et celui **de maintenir ces données exactes et complètes** au sein **d'une base de données spécialisée**. La référence à **l'absence de redondance** traduit l'obligation prévue au paragraphe 6 de l'article 28 de la directive **d'éviter toute répétition inutile** de la collecte des données d'enregistrement de noms de domaine.

À cette fin, les offices et les bureaux d'enregistrement mettent en place **des procédures**, **accessibles au public**, permettant de **vérifier ces données lors de leur collecte** et **d'assurer la sécurité de leur base de données**, comme le prévoit le paragraphe 3 de l'article 28 qui dispose que les États membres exigent que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine aient mis en place **des politiques et des procédures** mises à la disposition du public, notamment **des procédures de vérification**, visant à **garantir que les bases de données contiennent des informations exactes et complètes**.

Un décret en Conseil d'État, pris après avis de **la Commission nationale informatique et libertés (Cnil)**, fixe **la liste des données** relatives aux noms de domaine devant être collectées.

Cette liste contiendra au moins les éléments prévus par le paragraphe 2 de l'article 28 de la directive NIS 2, à savoir **les informations nécessaires** pour **identifier** et **contacter les titulaires des noms de domaine** et **les points de contact** qui gèrent **les noms de domaine relevant des domaines de premier niveau**.

Il s'agit notamment des éléments suivants :

- le nom de domaine ;

- la date d'enregistrement ;

- le nom du titulaire, **l'adresse de courrier électronique** et **le numéro de téléphone** permettant de le contacter ;

- l'adresse de courrier électronique et **le numéro de téléphone** permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

III. La position de la commission – la transposition de la mesure clef de l'article 28 de la directive NIS 2 et un renvoi à un décret en Conseil d'État légitime

L'article 19 assure la transposition de la principale disposition de l'article 28 de la directive NIS 2, à savoir **l'obligation pour les offices et les bureaux d'enregistrement des noms de domaine de mettre en place une base de données** afin de **pouvoir accéder aux données permettant d'identifier le propriétaire d'un nom de domaine en cas d'incident**.

Le renvoi à un décret en Conseil d'État de la liste des données collectées, au demeurant largement prescrites par les dispositions de l'article 28 de la directive NIS 2, **ne pose pas de difficultés**, dès lors que ce décret fera l'objet **d'un avis de la Commission nationale informatique et libertés (Cnil)**, indispensable pour **encadrer précisément la protection des données personnelles**.

La commission a adopté cet article sans modification.

Article 20

Durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaines

Cet article définit la durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaines, en prévoyant que ceux-ci doivent conserver les données relatives à chaque nom de domaine dans leur base de données tant que le nom du domaine est utilisé.

La commission a adopté cet article sans modification.

I. La situation actuelle – une absence de précision dans la directive NIS 2 sur la durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaines

L'article 28 de la directive NIS 2 ne prévoit **pas explicitement de durée de conservation des données collectées** par les offices et les bureaux d'enregistrement des noms de domaines mais dans la mesure où ils sont **obligés de collecter ces données** et de **les maintenir exactes et complètes au sein d'une base de données spécialisée**, il paraît **logique et cohérent** de considérer que cette obligation demeure **valable uniquement tant que le nom de domaine est utilisé**.

II. Le dispositif envisagé – une conservation des données relatives à chaque nom de domaine tant que le nom de domaine est utilisé

L'article 20 prévoit que les offices d'enregistrement des noms de domaines et les bureaux d'enregistrement des noms de domaines **conservent les données relatives à chaque nom de domaine dans leur base de données tant que le nom de domaine est utilisé**.

III. La position de la commission – un dispositif cohérent avec les dispositions de l'article 28 de la directive NIS 2

Le dispositif proposé par le présent article paraît **cohérent avec les dispositions de l'article 28** de la directive NIS 2 et propose **une durée de conservation conforme à ses objectifs**.

Il n'appelle donc pas de modification de son texte par la commission spéciale.

La commission a adopté cet article sans modification.

Article 21

Obligation de publication des données d'enregistrement d'un nom de domaine

Cet article oblige les offices et bureaux d'enregistrement à publier sans retard les données d'enregistrement relatives à un nom de domaine qui ne sont pas des données à caractère personnel.

La commission a adopté cet article sans modification.

I. La situation actuelle – l'article 28 de la directive NIS 2 prévoit une publication des données d'enregistrement relatives à un nom de domaine qui ne sont pas des données à caractère personnel

Le paragraphe 4 de l'article 28 de la directive NIS 2 prévoit que les États membres exigent que **les registres des noms de domaine de premier niveau** et **les entités fournissant des services d'enregistrement de noms de domaine** rendent **publiques**, sans retard injustifié après l'enregistrement d'un nom de domaine, **les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel**.

II. Le dispositif envisagé – une transposition littérale des dispositions de l'article 28 de la directive NIS 2

Le présent article 21 du projet de loi prévoit que **les offices d'enregistrement des noms de domaine** et **les bureaux d'enregistrement des noms de domaine** rendent **publiques** sans retard injustifié après l'enregistrement d'un nom de domaine, **les données d'enregistrement relatives à ce nom de domaine, dès lors qu'elles n'ont pas de caractère personnel**.

L'article 21 propose donc **une transposition quasiment mot pour mot** du paragraphe 4 de l'article 28 de la directive.

III. La position de la commission – un dispositif qui ne pose pas de difficultés dès lors que la protection des données personnelles est bien assurée

Cette transposition très littérale de la directive ne présente **pas de difficultés**, dès lors qu'elle a **bien conservé la restriction en faveur de la protection des données à caractère personnel**, raison pour laquelle la commission l'a adopté sans modification.

La commission a adopté cet article sans modification.

Article 22

Obligation de communiquer les données collectées par les offices et bureaux d'enregistrement à l'autorité judiciaire et à l'Anssi pour les besoins des procédures pénales ou de la sécurité des systèmes d'information

Cet article prévoit que les offices et les bureaux d'enregistrement devront mettre en place des procédures permettant aux services de l'État (autorité judiciaire et autorité nationale de sécurité des systèmes d'information) d'accéder aux données collectées relatives aux noms de domaine, à leur demande, dans un délai maximal de 72 heures.

La commission a adopté cet article sans modification.

I. La situation actuelle – l'article 28 de la directive NIS 2 prévoit un droit d'accès des autorités légitimes aux données collectées par les offices et bureaux d'enregistrement

Le paragraphe 5 de l'article 28 de la directive NIS 2 prévoit que les États membres imposent **aux registres des noms de domaine de premier niveau** et **aux entités fournissant des services d'enregistrement de noms de domaine** de **donner accès aux données spécifiques d'enregistrement de noms de domaine sur demande légitime** et **dûment motivée des demandeurs d'accès légitimes**, dans le respect du droit de l'Union en matière de protection des données.

En outre, le paragraphe 5 prévoit que les États membres exigent que **les registres des noms de domaine de premier niveau** et **les entités fournissant des services d'enregistrement de noms de domaine** répondent **sans retard injustifié** et en tout état de cause **dans un délai de 72 heures** après réception de toute demande d'accès.

Enfin, il précise que les États membres imposent que **les politiques** et **procédures de divulgation de ces données** soient **rendues publiques**.

II. Le dispositif envisagé – les offices et les bureaux d'enregistrement devront mettre en place des procédures permettant à l'autorité judiciaire et à l'Anssi d'accéder aux données collectées relatives aux noms de domaine

Le premier alinéa de l'article 22 du projet de loi prévoit que pour **les besoins des procédures pénales** et de **la sécurité des systèmes d'information**, **les agents habilités** à cet effet par **l'autorité judiciaire** ou par **l'autorité nationale de sécurité des systèmes d'information** (c'est-à-dire l'Anssi) peuvent **obtenir** des offices et bureaux d'enregistrement **les données** relatives à **chaque nom de domaine**, données que ces derniers **conservent dans leur**

base de données tant que le nom de domaine est utilisé, conformément aux dispositions de l'article 20.

Alors que le paragraphe 5 de l'article 28 de la directive prévoit que les données spécifiques d'enregistrement de noms de domaines doivent être fournis « *sur demande légitime et dûment motivée des demandeurs d'accès légitimes* », la transposition vient donc préciser qu'une demande légitime et dûment motivée devra correspondre aux « *besoins **des procédures pénales** et de **la sécurité des systèmes d'information*** » et que les « *demandeurs d'accès légitimes* » seront uniquement « ***les agents habilités à cet effet par l'autorité judiciaire ou par l'Anssi*** ».

Le deuxième alinéa de l'article 22 prévoit que les offices et les bureaux d'enregistrement fixent **les règles de procédure pour la communication de ces données** aux agents habilités à cet effet par l'autorité judiciaire ou par l'Anssi. Cette communication intervient **dans un délai n'excédant pas 72 heures**. Ces règles sont **accessibles au public**.

Le paragraphe 5 de l'article 28 prévoit effectivement que les offices et les bureaux d'enregistrement « *répondent **sans retard injustifié** et en tout état de cause **dans un délai de 72 heures** après réception de toute demande d'accès* ». Mais il ne précisait pas que **les règles de procédure pour la communication des données aux agents habilités à cet effet serait fixée par les offices et les bureaux d'enregistrement**.

La référence à **la publicité des règles qui doivent être accessibles au public** transpose l'alinéa de l'article 5 qui prévoit que « *les États membres imposent que les politiques et procédures de divulgation de ces données soient rendues publiques* ».

Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés (Cnil) fixe les modalités d'application de cet article 22.

III. La position de la commission – une mesure de transposition qui établit clairement et de façon limitative les autorités susceptibles d'avoir accès aux données relatives aux noms de domaine

Comme les articles précédents de la section 3 « Enregistrement des noms de domaine », cet article 22 assure **une transposition fidèle d'une disposition de l'article 28 de la directive NIS 2**, en précisant les autorités légitimes à demander les données relatives aux noms de domaine, qui sont logiquement **l'autorité judiciaire** pour **le besoin des procédures pénales** et **l'Anssi** pour **la sécurité des systèmes d'information**, ce qui permet de **limiter strictement leur nombre**.

Le renvoi à un décret en Conseil d'État de ses modalités d'application **ne pose pas de difficultés**, l'avis de la Cnil permettant de garantir **le respect de la réglementation sur les données personnelles**.

La commission a adopté cet article sans modification.

Article 23

Dérogation aux secrets protégés par la loi pour la communication d'informations en matière de cybersécurité entre l'Anssi et plusieurs de ses interlocuteurs

Cet article vise à déroger aux secrets protégés par la loi et au secret de l'instruction pour la communication d'informations en matière de cybersécurité entre l'Anssi et plusieurs de ses interlocuteurs.

La commission a adopté cet article modifié par un amendement prévoyant que la communication d'informations effectuée ne peut intervenir que si elle est nécessaire à l'accomplissement des missions des personnes émettrices ou destinataires de ces informations.

I. La situation actuelle – la directive NIS 2 prévoit la possibilité d'échanger des informations confidentielles pour assurer son application

Le paragraphe 13 de l'article 2 de la directive NIS 2 prévoit que, sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne (TFUE), **les informations considérées comme confidentielles** en application de la réglementation de l'Union ou nationale des États membres, telle que **les règles applicables au secret des affaires**, **ne peuvent faire l'objet d'un échange** avec la Commission européenne et d'autres autorités concernées conformément à la directive **que si cet échange est nécessaire à l'application de la directive**.

Mais cela signifie bien que c**es informations confidentielles peuvent effectivement faire l'objet d'échanges** pour permettre **l'application de la directive**.

Étant confidentielles, ces informations échangées **se limitent au minimum nécessaire** et sont **proportionnées à l'objectif de cet échange**.

Cet échange **d'informations préserve la confidentialité des informations concernées** et **protège la sécurité** et **les intérêts commerciaux des entités concernées**.

Le paragraphe 14 de l'article 2 précise que les entités, les autorités compétentes, les points de contact uniques et les CSIRT **traitent les données à caractère personnel** dans la mesure nécessaire aux fins de la directive et conformément au règlement (UE) 2016/679, plus connu sous **le nom de règlement général sur la protection des données (RGPD).**

Le traitement des données à caractère personnel en vertu de la directive par **les fournisseurs de réseaux de communications électroniques publics** ou **les fournisseurs de services de communications électroniques accessibles au public** est également effectué conformément au droit de

l'Union en matière **de protection des données** et au droit de l'Union en matière **de protection de la vie privée**.

À noter enfin que le paragraphe 11 de l'article 2 prévoit que les obligations énoncées dans la directive **n'impliquent pas la fourniture d'informations** dont **la divulgation** serait **contraire aux intérêts essentiels des États membres** en matière **de sécurité nationale**, **de sécurité publique** ou **de défense**.

II. Le dispositif envisagé – la définition d'un cadre en matière de coopération et d'échange d'informations en matière de cybersécurité

Afin d'assurer la transposition du paragraphe 13 de l'article 2 de la directive, l'article 23 vise :

- à **définir un cadre** en matière **de coopération** et **d'échange d'informations** en matière **de cybersécurité** ;
- dans cette perspective, à **déroger aux secrets protégés par la loi** et **au secret de l'instruction** ;
- mais, dans le même temps, à **apporter des garanties suffisantes à la sécurité nationale**, **la sécurité publique** ou **la défense nationale**.

En conséquence, l'article 23 prévoit que les dispositions de l'article 11 du code de procédure pénale, qui portent sur **le secret de l'instruction**, ou celles relatives **aux secrets protégés par la loi** ne font **pas obstacle à la communication d'informations** dont ils disposent aux fins de l'accomplissement de leurs missions respectives entre d'une part **l'autorité nationale de la sécurité des systèmes d'information** (c'est-à-dire l'Anssi) et, d'autre part :

- **La Commission nationale de l'informatique et des libertés** (Cnil) ;
- **Les autorités compétentes** chargées de **la gestion des risques en matière de cybersécurité** en vertu **d'un acte sectoriel de l'Union européenne** ;
- **Les autorités chargées de la politique pénale**, **de l'action publique et de l'instruction**. Cette coopération est justifiée par **la lutte contre la cybercriminalité** ;
- **La Commission européenne** ;
- Les autorités compétentes **des autres États membres de l'Union européenne** ;
- **Des centres de réponse aux incidents de sécurité informatique** (les CSIRT) ;

- **Des organismes internationaux** concourant **aux missions de sécurité** ou **de défense des systèmes d'information**.

Ces entités peuvent **se communiquer librement les informations dont elles disposent** et **se consulter mutuellement** aux fins de **l'accomplissement de leurs missions respectives**, **à l'exception** des informations dont la communication porterait **atteinte à la sécurité publique**, **à la défense** et **la sécurité nationale** ou **à la conduite des relations internationales**.

Cela **exclut donc explicitement la communication d'informations couvertes par le secret de la défense nationale**, conformément à ce que prévoit le paragraphe 11 de l'article 2 de la directive NIS 2.

En revanche, comme le prévoit tout aussi explicitement le paragraphe 13 de l'article 2 de la directive NIS 2, ces dispositions **peuvent impliquer la communication d'informations relevant du secret des affaires**, dont la protection est fondée sur les articles L. 151-1 et suivants du code de commerce.

L'article L. 151-1 du code de commerce définit la notion **d'information protégée au titre du secret des affaires** selon trois critères :

- cette information n'est **pas généralement connue** ou a**isément accessible** pour les personnes familières de ce type d'informations ;
- elle revêt **une valeur commerciale**, **effective ou potentielle**, du fait **de son caractère secret** ;
- elle fait l'objet de la part de son détenteur légitime **de mesures de protection raisonnables**, pour **en conserver le caractère secret**.

En outre, les informations échangées peuvent contenir **des données à caractère personnel** comme le prévoit le paragraphe 14 de l'article 2.

L'article 23 **ne liste pas l'intégralité des secrets protégés par la loi** auxquels sont apportés une dérogation mais mentionne les « *autres secrets protégés par la loi* »[1].

Cette formulation est liée **au risque d'enchevêtrement des secrets protégés par la loi applicables à une même information partagée** entre les différentes entités listées par l'article en question.

Or, le paragraphe 13 de la directive NIS 2 prévoit **une dérogation aux secrets protégés par la législation nationale** dès lors que **l'échange de ces informations est nécessaire à l'application de la directive**.

---

[1] *La formulation mentionnant les* « autres secrets protégés par la loi » *existe déjà au niveau législatif, à l'article L. 311-5 du code des relations entre le public et l'administration :* « 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte : *[…]* h) Ou sous réserve de l'article L. 124-4 du code de l'environnement, aux autres secrets protégés par la loi »

Tous les secrets protégés par la loi sont donc concernés. Il sera par exemple possible de **déroger au secret professionnel auquel sont astreints les agents publics**, en application de l'article L. 121-6 du code général de la fonction publique.

Le deuxième alinéa de l'article 23 prévoit que ses modalités d'application, notamment **les modalités du partage d'informations**, sont déterminées par décret en Conseil d'État.

III. La position de la commission – des modalités de partage d'information confidentielles proportionnées à leur objectif et respectueuses des impératifs de la défense nationale

Afin de **prévenir les menaces cyber**, de **résoudre les incidents en cas d'attaque** ou bien encore de **lutter contre la cybercriminalité**, **le partage d'informations confidentielles** entre **les autorités légitimes et habilitées à cette fin** constitue **une nécessité**. En conséquence, **ce partage d'informations confidentielles** est prévu par **la directive NIS 2**.

Un certain nombre de ces informations confidentielles étant explicitement **couvertes par des secrets protégés par la loi**, le présent projet de loi de transposition doit prévoir **quelles autorités** pourront légitimement **contribuer à ce partage d'informations confidentielles** dans le but **d'appliquer la directive NIS 2** et dans quelles conditions.

Dans la mesure où **la liste des autorités appelées à partager des informations confidentielles en matière de cybersécurité** mentionnées au présent article 23 du projet de loi **paraît cohérente** et où **les informations dont la communication** porterait **atteinte à la sécurité publique**, **à la défense et la sécurité nationale** ou **à la conduite des relations internationales** ne pourront **pas faire l'objet d'échanges**, le dispositif prévu par le présent article 23 apparaît à la fois **pleinement compatible avec les objectifs de la directive** et **respectueux des impératifs de la défense nationale**.

La commission spéciale a toutefois adopté deux amendements identiques COM 54 et COM 70 présentés respectivement par Catherine Morin-Dessailly et Vanina Paoli-Gagin pour prévoir que la communication d'informations effectuée en vertu du présent article 23 ne peut intervenir **que si elle est nécessaire à l'accomplissement des missions des personnes émettrices ou destinataires de ces informations**. Les informations échangées se limitent **au minimum nécessaire** et sont **proportionnées à l'objectif du partage**. Le partage d'informations préserve **la confidentialité des informations concernées** et protège **la sécurité et les intérêts commerciaux** des entités concernées.

La commission a adopté cet article ainsi modifié.

Article 24

Agrément par l'Anssi d'organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents cyber

Cet article permet à l'Anssi d'agréer des organismes publics ou privés en tant que relais de son action dans la prévention et la gestion des incidents de cybersécurité.

La commission a adopté cet article sans modification.

I. La situation actuelle – un réseau de CSIRT relais en cours de structuration pour démultiplier les capacités d'action de l'Anssi

Cet article 24 s'inscrit en complément de l'article 17 qui prévoit, en transposition de l'article 23 de la directive NIS 2, **les obligations de notifications d'incidents importants** auxquels sont soumises les entités « essentielles » et « importantes ».

Il ne transpose donc pas directement lui-même une disposition précise de la directive NIS 2 mais participe à **la structuration du réseau de *computer security incident response team* (CSIRT)** placés **sous l'autorité de l'Agence nationale de sécurité des systèmes d'information (Anssi)** pour **prévenir** et **gérer les incidents de cybersécurité**.

L'Anssi a en effet soutenu ces dernières années **la création de CSIRT relais au niveau ministériel**, **sectoriel** et **territorial**, afin de **démultiplier ses capacités en matière de réponse aux incidents de sécurité informatique**.

II. Le dispositif envisagé – la mise en place d'un dispositif d'agrément destiné à renforcer la légitimité des CSIRT relais et à autoriser les échanges d'informations couvertes par des secrets protégés par la loi avec l'Anssi

Le premier alinéa de l'article 24 prévoit que **l'autorité nationale de sécurité des systèmes d'information** (c'est-à-dire l'Anssi) **agrée des organismes publics ou privés** en tant que **relais** dans **la prévention et la gestion des incidents de cybersécurité**.

Il dispose également que l'Anssi et les organismes qu'elle a ainsi agréés sont autorisés à **échanger entre eux des informations couvertes par des secrets protégés par la loi**.

Le deuxième alinéa prévoit que les modalités d'application de cet article 24, notamment **les modalités de dépôt et d'examen des demandes d'agrément des organismes publics ou privés agréés par l'Anssi**, sont déterminés par décret en Conseil d'État.

Cet article vise à disposer **d'une base législative solide** pour **consolider** et **structurer** encore davantage **le réseau de CSIRT relais de**

l'action de l'Anssi que celle-ci a commencé à mettre en place ces dernières années pour **accroître l'impact de son action**.

Le dispositif d'agrément prévu au présent article 24 vise en effet à **donner aux CSIRT relais une légitimité** et **un cadre pour l'accompagnement des entités régulées**, tout en préservant **le rôle de coordination globale de l'Anssi**.

Le directeur général de l'Anssi a indiqué à la commission spéciale que **le rôle de ces CSIRT relais vis-à-vis des entités régulées** au titre de la directive NIS 2 serait le suivant :

- contribuer au **partage de l'information opérationnelle** émise par l'Agence **en relayant les éléments pertinents** à leurs bénéficiaires ;
- relayer **les alertes** et **les campagnes de signalement des vulnérabilités** de l'Agence et contribuer à **la recherche de compromissions** auprès de leurs bénéficiaires ;
- orienter **les actions de réponse à incident** d'une entité accompagnée par un ou plusieurs prestataires, en coordination avec l'Anssi, afin d'assurer **une synchronisation opérationnelle** ;
- accompagner les entités régulées à **la déclaration de l'incident auprès de l'Agence**, ainsi que pour **toutes les déclarations obligatoires** (ex : Cnil) ou pour **le dépôt de plainte** ;
- établir **les statistiques des incidents cyber sur leur périmètre** et **les partager au profit de la communauté des CSIRT**, afin d'affiner **la connaissance de la menace cyber à l'échelle nationale**.

Il est en revanche clairement établi que **c'est l'Anssi**, et non les CSIRT relais sectoriels, **qui sera destinataire des notifications d'incidents importants** prévues à l'article 17 du présent projet de loi, les CSIRT relais ayant uniquement **un rôle d'accompagnement et de facilitation** auprès des entités régulées.

III. La position de la commission – compte tenu du changement d'échelle induit par NIS 2, la consolidation d'un réseau de relais de l'action de l'Anssi constitue une nécessité

L'entrée en vigueur du titre II du présent projet de loi transposant la directive NIS 2 constituera **un changement d'échelle considérable** pour les missions de l'Anssi avec le passage d'environ **500 entités régulées** au titre de NIS 1 à **15 000 entités régulées** au titre de NIS 2.

Si l'Anssi affectera **une cinquantaine d'équivalents temps plein (ETP) à son rôle de supervision**, la nécessité pour elle de disposer, dans tous les secteurs « hautement critiques » et « critiques », et partout sur le territoire, **de relais**, est **indispensable**.

Ce travail a déjà largement été entamé ces dernières années avec **la structuration progressive d'un réseau de CERT relais** qui doit maintenant **prendre une nouvelle dimension** avec la mise en application de la transposition de la directive NIS 2.

Le fait de les agréer **renforcera leur légitimité vis-à-vis de leur écosystème sectoriel** et les aidera à devenir **des acteurs clefs de l'accompagnement** dans **la montée en gamme en matière de cybersécurité** des entreprises, des administrations et des collectivités territoriales.

En ce qui concerne les CSIRT relais régionaux, ils pourront en outre contribuer, au niveau local, à **développer une filière cyber**, via **la valorisation de prestataires de confiance auprès de clients potentiels**, et à **renforcer l'attractivité des territoires** où la présence de prestataires cyber de proximité deviendra **une garantie de sécurité pour les acteurs économiques**.

Le renvoi à un décret en Conseil d'État des modalités de dépôt et d'examen des demandes d'agrément des CSIRT relais **ne soulevant pas de difficultés**, la commission spéciale n'a pas souhaité amender le présent article 24.

La commission a adopté cet article sans modification.

CHAPITRE III
DE LA SUPERVISION

Article 25
Prescription par l'Anssi de mesures nécessaires en cas de menace pour la sécurité des systèmes d'information de plusieurs types d'entités

Cet article vise à autoriser l'Anssi à prescrire des mesures à diverses entités lorsqu'elle aura connaissance d'une menace susceptible de porter atteinte à la sécurité de leurs systèmes d'information.

La commission a adopté un amendement rédactionnel.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle - des obligations de notification des incidents cyber pèsent déjà sur diverses entités, certaines d'entre elles pouvant se voir imposer la mise en œuvre de mesures en cas de crise

1. L'Anssi doit être informée des incidents significatifs affectant les systèmes d'information des opérateurs de services essentiels (OSE)

Depuis la transposition par le législateur de la directive européenne NIS 1[1] en 2018, **le Premier ministre fixe les règles de sécurité nécessaires à la protection des réseaux et systèmes d'information** nécessaires à la fourniture de services essentiels par les **opérateurs de services essentiels (OSE)**, de façon à garantir **un niveau de sécurité adapté au risque existant**, compte tenu de l'état des connaissances[2].

Ces règles définissent **les mesures appropriées** pour **prévenir les incidents qui compromettent la sécurité des réseaux** et **systèmes d'information** utilisés pour **la fourniture des services essentiels** ou pour **en limiter l'incidence** afin d'assurer **la continuité de ces services**. Les opérateurs concernés par ces règles les appliquent **à leurs frais**.

En outre, les OSE doivent **déclarer à l'Anssi**, sans délai après en avoir pris connaissance, **les incidents affectant les réseaux et systèmes d'information** nécessaires à **la fourniture de services essentiels**, lorsque ces incidents ont ou sont susceptibles d'avoir, compte tenu du nombre

---

[1] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.*

[2] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 6 ; décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, article 10 ; arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, annexe.*

d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, **une incidence significative sur la continuité de ces services**[1].

En cas de manquement à cette obligation, les dirigeants d'un OSE sont passibles d'**une amende de 75 000 euros**[2].

Les fournisseurs de service numérique sont soumis à **des obligations et à un régime de sanctions similaires**[3].

2. Les opérateurs d'importance vitale (OIV) sont astreints au respect d'une obligation similaire et peuvent se voir imposer des mesures jugées nécessaires en cas de crise majeure

Depuis l'entrée en vigueur de la loi de programmation militaire pour les années 2014 à 2019[4], **le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale (OIV)** et des opérateurs publics ou privés qui participent à ces systèmes dont une atteinte à la sécurité ou au fonctionnement risquerait de **diminuer d'une façon importante le potentiel de guerre ou économique**, **la sécurité** ou **la capacité de survie de la Nation** ou pourrait **présenter un danger grave pour la population**[5]. Les entités concernées sont tenues d'appliquer ces règles **à leurs frais**.

Dans ce cadre, le législateur a institué une obligation pour les OIV d'**informer sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information** concernés[6].

Au surplus, le Premier ministre est autorisé, pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, à **décider des mesures que les OIV doivent mettre en œuvre**[7].

3. La directive NIS 2 impose aux États membres de veiller à la mise en œuvre par les entités essentielles et importantes des mesures nécessaires à la gestion des risques cyber

L'article 21 de la directive dite NIS 2 prévoit que les États membres veillent à ce que les entités « essentielles » et « importantes » prennent **les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux**

---

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 7 ; décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, article 11.*

[2] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 9.*

[3] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, articles 10 à 15.*

[4] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, article 22.*

[5] *Article L. 1332-6-1 du code de la défense.*

[6] *Article L. 1332-6-2 du code de la défense.*

[7] *Article L. 1332-6-4 du code de la défense.*

et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour **éliminer ou réduire les conséquences** que **les incidents ont sur les destinataires de leurs services et sur d'autres services**.

Si la traduction de cette obligation est avant tout portée par l'article 14 du présent projet de loi, l'article 25 confère également **des pouvoir à l'autorité nationale de sécurité des systèmes d'information** (c'est-à-dire l'Anssi) lorsqu'elle a **connaissance d'une menace** susceptible **de porter atteinte aux entités régulées au titre de la directive NIS 2**.

II. Le dispositif proposé - la possibilité pour l'Anssi d'imposer à plusieurs catégories d'entités la mise en œuvre de mesures en cas de menace pour la sécurité de leurs systèmes d'information

Le présent article 25 prévoit d'habiliter l'Anssi, lorsqu'elle aura connaissance **d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information de diverses entités**, à **prescrire à l'entité concernée les mesures nécessaires, notamment pour éviter un incident ou y remédier**, ainsi que **le délai qui leur sera accordé** pour mettre en œuvre ces mesures et **en rendre compte**.

Les entités concernées seront **les personnes mentionnées à l'article 14** du présent projet de loi, à savoir :

- les entités « essentielles » ;

- les entités « importantes » ;

- les administrations de l'État et **leurs établissements publics administratifs** qui exercent leurs activités dans **les domaines de la sécurité publique**, **de la défense** et **de la sécurité nationale** ainsi que **de la répression pénale** ;

- les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information ;

- le Commissariat à l'énergie atomique et aux énergies alternatives pour ses activités dans le domaine de la défense ;

- les juridictions administratives et judiciaires.

Les bureaux d'enregistrement pourraient également se voir prescrire la mise en œuvre de mesures par l'Anssi.

Un décret en Conseil d'État devrait déterminer **les modalités d'application de ces dispositions**.

Pour rappel, conformément à l'article 23 de la directive NIS 2 , l'article 17 du présent projet de loi tend par ailleurs à obliger les mêmes entités – à l'exception des bureaux d'enregistrement – à **notifier sans retard injustifié**

à l'Anssi tout incident ayant une incidence importante sur la fourniture de leurs services.

III. La position de la commission - des modifications rédactionnelles

Constatant qu'il se bornait à transposer les dispositions de la directive NIS 2, la commission spéciale a adopté le présent article modifié par un **amendement rédactionnel n° COM-107** des rapporteurs.

En tout état de cause, le renvoi à un décret en Conseil d'État pour la détermination des modalités de son application paraît **justifié** par le caractère manifestement réglementaire des précisions à apporter, en ce qui concerne tant la procédure à suivre que les délais de mise en œuvre des mesures prescrites.

La commission a adopté cet article ainsi modifié.

SECTION 1
RECHERCHE ET CONSTATATION DES MANQUEMENTS

SOUS-SECTION 1
HABILITATION

Article 26
Habilitation des agents de plusieurs organismes à rechercher et constater les manquements et infractions en matière de cybersécurité

Cet article vise à permettre aux agents de l'Anssi, ainsi que des organismes indépendants et des services de l'État spécialement désignés, de rechercher et constater les manquements à la réglementation et les infractions en matière de cybersécurité.

La commission a adopté un amendement clarifiant notamment le rôle des agents et personnels des organismes indépendants en matière de recherche de manquements aux obligations qui s'imposent aux personnes contrôlées.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle - l'extension des compétences de l'Anssi et d'autres entités dans le champ du contrôle

Dans le cadre **des nouvelles obligations** imposées ces dernières années **aux entités concernées par la réglementation européenne en matière de cybersécurité**, l'Agence nationale de la sécurité des systèmes d'information (Anssi) s'est vue attribuer **des missions supplémentaires**.

En premier lieu, pour l'application **du règlement dit « eIDAS » de 2014**[1], l'Anssi assure désormais un **triple rôle** en matière **de contrôle de la sécurité des moyens d'identification électronique** :

- **un rôle de certification**, qui s'exerce au travers, d'une part, de **la certification de la conformité des moyens d'identification électronique aux exigences du cahier des charges établi par l'Anssi –** correspondant an niveau de garantie « élevé » au sens de la réglementation européenne[2] **–**, qui induit la **présomption de fiabilité**, et, d'autre part, de **la délivrance aux prestataires fournissant un moyen d'identification électronique autre que présumé fiable** et qui en font la demande **d'une certification attestant du niveau de**

[1] *Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE.*

[2] *Article R. 54-16 du code des postes et des communications électroniques.*

garantie présenté par ce moyen d'identification électronique, sur la base de **référentiels** définissant les exigences de sécurité associées[1] ;

- un **rôle de publication** sur son site internet **des décisions de certification en cours de validité** sous la forme d'une « liste nationale de confiance »[2] ;

- et un **rôle de contrôle**, soit **par ses propres moyens**, soit **par le biais d'un centre d'évaluation**, **du respect par le prestataire de confiance des exigences induites par la certificatio**n pendant la période de validité de la décision de certification[3].

Par ailleurs, le règlement dit « *Cyber Security Act* » (CSA) fait obligation à chaque État membre de l'Union européenne de désigner une ou plusieurs **autorités nationales de certification de cybersécurité (ANCC)**, rôle qui incombe, en France, **à l'Anssi**[4].

Cette dernière doit ainsi, entre autres, **superviser et faire respecter les règles prévues dans les schémas européens de certification de cybersécurité** et contrôler le respect des obligations qui incombent aux fabricants ou fournisseurs de produits, services ou processus technologiques de l'information et de la communication.

II. Le dispositif proposé – une habilitation des agents de l'Anssi et d'autres entités à rechercher et à constater les manquements et infractions en matière de cybersécurité

Le présent article **habilite les agents et personnes, spécialement désignés et assermentés à cet effet, de l'Anssi et des organismes indépendants ou services de l'État qu'elle désigne, à rechercher et à constater les manquements et infractions** aux obligations prévues par :

- **le règlement dit « eIDAS »** de 2014 ;

- **le règlement dit « CSA »** de 2019 ;

- **les chapitres II et III du titre II du présent projet de loi**, respectivement consacrés à la cyber résilience et à la supervision ;

- les articles L. 100, L. 102 et L. 103 du code des postes et des communications électroniques, lesquels portent respectivement sur **les obligations incombant aux prestataires d'envois recommandés**

---

[1] *Article L. 102 du code des postes et des communications électroniques ; décret n° 2022-1004 du 15 juillet 2022 fixant les modalités de certification de moyens d'identification électronique ainsi que le cahier des charges permettant d'établir la présomption de fiabilité de ces moyens.*

[2] *Article R. 54-13 du code des postes et des communications électroniques.*

[3] *Article R. 54-13 du code des postes et des communications électroniques.*

[4] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'Enisa (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013, article 58.*

électroniques, **les caractéristiques des moyens d'identification électronique** ainsi que **les modalités de leur certification** (*voir supra*) et **les caractéristiques des services de coffre-fort numérique** et **la possibilité de leur certification**.

- et **les exigences de cybersécurité résultant des autorisations**, **certifications**, **qualifications** et **agréments** que l'Anssi délivre.

III. La position de la commission - des clarifications nécessaires

Jugeant cet article justifié par la nécessité de permettre aux agents et personnels de l'Anssi de conduire les opérations de contrôle dont ils sont chargés, la commission spéciale a adopté **un amendement n° COM-109** des rapporteurs.

Celui-ci **supprime la référence aux infractions** pouvant avoir été commises par les personnes contrôlées par l'Anssi, compte tenu du remplacement du régime de sanctions pénales actuellement en vigueur par un régime d'amendes administratives, et clarifie le rôle des agents et personnels des organismes indépendants en matière de recherche des manquements.

Leur intervention serait ainsi limitée à la **recherche des manquements** aux obligations qui s'imposent aux personnes contrôlées, sous le contrôle des agents et personnels assermentés de l'Anssi ou des services de l'État désignés par elle. Ils ne seraient eux-mêmes **ni assermentés ni habilités à constater lesdits manquements**, c'est-à-dire à en dresser procès-verbal.

La commission spéciale a également adopté un **amendement de coordination n° COM-108** créant un article additionnel avant le présent article.

La commission a adopté cet article ainsi modifié.

SOUS-SECTION 2
DES POUVOIRS

Article 27
Droits et obligations des agents chargés d'un contrôle de l'Anssi et de la personne contrôlée

Cet article vise à préciser le cadre dans lequel doivent se dérouler les contrôles de l'Anssi en fixant les droits et obligations des agents chargés du contrôle et des personnes contrôlées.

La commission a adopté un amendement procédant à des modifications rédactionnelles et de sécurisation juridique.

La commission a adopté cet article ainsi modifié.

I. Les modifications proposées par le Gouvernement : la détermination des droits et obligations des agents chargés d'un contrôle de l'Anssi et des personnes contrôlées

A. La réglementation permet le contrôle de la sécurité des systèmes d'information des opérateurs de services essentiels et des opérateurs d'importance vitale, sans en fixer le cadre avec précision

Les opérateurs de services essentiels (OSE) peuvent être soumis par le Premier ministre à **des contrôles destinés à vérifier le respect de leurs obligations en matière de sécurité des réseaux et systèmes d'information** ainsi que le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de services essentiels[1].

Le contrôle est effectué, sur pièces et sur place, par l'Agence nationale de la sécurité des systèmes d'information (Anssi) ou par des prestataires de service qualifiés par le Premier ministre, **son coût étant à la charge des OSE**.

Dans ce cadre, les OSE sont **tenus de communiquer** à l'Anssi ou au prestataire de service chargé du contrôle **les informations et éléments nécessaires à la réalisation du contrôle**, y compris les documents relatifs à leur politique de sécurité et, le cas échéant, les résultats d'audit de sécurité, et de leur permettre d'accéder aux réseaux et systèmes d'information faisant l'objet du contrôle afin d'effectuer des analyses et des relevés d'informations techniques.

En cas de manquement constaté à l'occasion d'un contrôle, l'Anssi peut mettre en demeure les dirigeants de l'OSE concerné de se conformer, dans un délai qu'elle détermine en tenant compte des conditions de

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 8.*

fonctionnement de l'OSE et des mesures à mettre en œuvre, aux obligations qui lui incombent.

Le fait, pour les dirigeants d'un OSE, de ne pas se conformer aux règles de sécurité qui s'imposent à eux à l'issue du délai fixé par la mise en demeure est puni de **100 000 € d'amende**[1]. Ils encourent par ailleurs **une amende de 125 000 €** s'ils font obstacle aux opérations de contrôle.

Les modalités de contrôle de la sécurité des systèmes d'information des opérateurs de services essentiels

Le Premier ministre, après avis des ministres concernés, notifie aux OSE sa décision d'imposer un contrôle du niveau de sécurité et du respect de leurs obligations en matière de sécurité des réseaux et systèmes d'information[2]. Il précise les objectifs et le périmètre du contrôle, fixe le délai dans lequel celui-ci est réalisé et indique, en fonction de la nature des opérations à mener, l'entité qui est en chargée.

Il n'est pas possible d'imposer à un OSE plus d'un contrôle par année civile d'un même réseau et système d'information, sauf si celui-ci est affecté par un incident de sécurité ou si des vulnérabilités ou des manquements aux règles de sécurité ont été constatés lors d'un contrôle précédent.

Pour la réalisation du contrôle, **l'OSE conclut une convention avec l'Anssi ou le prestataire de service chargé du contrôle** afin de déterminer les objectifs et le périmètre du contrôle, les modalités de déroulement du contrôle et les délais dans lequel il est réalisé, les conditions dans lesquelles l'Anssi ou le prestataire de service accède aux réseaux et systèmes d'information et effectue les analyses et les relevés d'informations techniques, les informations et éléments, notamment la documentation technique des matériels et des logiciels, que l'opérateur communique à l'Anssi ou au prestataire de service pour la réalisation du contrôle, ainsi que les conditions de protection de la confidentialité des informations traitées dans le cadre du contrôle[3]. Lorsque le contrôle est effectué par un prestataire de service, une copie de la convention signée doit être adressée sans délai par l'OSE à l'Anssi.

À l'issue du contrôle, **l'Anssi ou le prestataire de service rédige un rapport exposant ses constatations**, au regard de l'objectif du contrôle, sur le respect des obligations en matière de sécurité des réseaux et systèmes d'information et sur le niveau de sécurité des réseaux et systèmes d'information contrôlés[4]. Les vulnérabilités et les manquements aux règles de sécurité constatés lors du contrôle sont indiqués dans le rapport, qui formule le cas échéant **des recommandations pour y remédier**.

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 9.*
[2] *Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, article 13.*
[3] *Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, article 14.*
[4] *Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, article 15.*

L'Anssi ou le prestataire de service met l'OSE **en mesure de faire valoir ses observations**. Lorsque le contrôle est réalisé par un prestataire de service, celui-ci communique, dans le délai fixé pour la réalisation du contrôle, le rapport à l'Anssi. Cette dernière peut auditionner, dans un délai de deux mois à compter de la remise du rapport, le prestataire de service, en présence de l'OSE, si celui-ci a formulé des observations ou si elle l'y convie, et d'un représentant des ministres concernés si ceux-ci en ont exprimé le souhait, pour examiner les constatations et les recommandations figurant dans le rapport. **L'Anssi communique aux ministres concernés les conclusions du contrôle**.

De même, dans le cadre de la loi de programmation militaire pour les années 2014 à 2019[1], le législateur a autorisé le Premier ministre à demander à l'Anssi, à des services de l'État désignés par lui ou à des prestataires de service qualifiés par lui de soumettre les opérateurs d'importance vitale (OIV) à **des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité nécessaires à la protection des systèmes d'information**[2].

Le cas échéant, **le coût du contrôle est supporté par l'opérateur concerné**.

Le fait, pour les dirigeants d'un OIV, de ne pas satisfaire à leurs obligations en la matière est puni d'**une amende de 150 000 €**, cette sanction étant précédée d'une mise en demeure[3].

Les modalités de contrôle de la sécurité des systèmes d'information des opérateurs d'importance vitale

Le Premier ministre, après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, notifie aux OIV sa décision d'imposer un contrôle du niveau de sécurité et du respect des règles de sécurité nécessaires à la protection des systèmes d'information[4]. Il précise les objectifs et le périmètre du contrôle, fixe le délai dans lequel celui-ci est réalisé et indique, en fonction de la nature des opérations à mener, l'entité qui en est chargée.

Il n'est pas possible d'imposer à un OIV plus d'un contrôle par année civile d'un même système d'information, sauf si ses systèmes d'information sont affectés par un incident de sécurité ou si des vulnérabilités ou des manquements aux règles de sécurité ont été constatés lors d'un contrôle précédent.

Dans le cas où le contrôle serait confié à un service de l'État ou à un prestataire de service, **l'OIV doit lui fournir les informations nécessaires pour évaluer la sécurité de ses systèmes d'information** et les moyens nécessaires pour

[1] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, article 22.*
[2] *Article L. 1332-6-3 du code de la défense.*
[3] *Article L. 1332-7 du code de la défense.*
[4] *Article R. 1332-41-12 du code de la défense.*

accéder à ces systèmes d'information et à l'ensemble de leurs composants afin de lui permettre de réaliser des analyses sur les systèmes[1].

Dans le même cas, **l'OIV conclut une convention avec le service de l'État ou le prestataire de service chargé du contrôle** afin de déterminer les systèmes d'information qui font l'objet du contrôle, les objectifs et le périmètre du contrôle, les modalités de déroulement du contrôle – notamment les conditions d'accès aux sites et aux systèmes d'information –, les informations nécessaires à la réalisation du contrôle, fournies par l'opérateur, et les conditions de leur protection, ainsi que les modalités selon lesquelles sont effectuées les analyses techniques sur les systèmes d'information[2]. Une copie de cette convention doit être adressée sans délai par l'OIV à l'Anssi.

Le service de l'État ou le prestataire de service ayant réalisé le contrôle rédige un rapport exposant ses constatations, au regard de l'objectif du contrôle, sur le niveau de sécurité des systèmes d'information contrôlés et le respect des règles de sécurité nécessaires à leur protection[3]. Les vulnérabilités et les manquements aux règles de sécurité constatés lors du contrôle sont indiqués dans le rapport, qui formule le cas échéant **des recommandations pour y remédier**. **Le rapport est couvert par le secret de la défense nationale**.

Après avoir mis l'OIV **en mesure de faire valoir ses observations**, le service de l'État ou le prestataire de service remet, dans le délai fixé pour la réalisation du contrôle, le rapport à l'Anssi. Cette dernière peut auditionner, dans un délai de deux mois à compter de la remise du rapport, le service de l'État ou le prestataire de service en question, le cas échéant en présence de l'OIV, aux fins d'examiner les constatations et les recommandations figurant dans le rapport. Elle peut inviter les ministres coordonnateurs des secteurs d'activités d'importance vitale concernés à assister à cette audition. En tout état de cause, **l'Anssi communique aux ministres coordonnateurs concernés les conclusions du contrôle**.

Qu'il s'agisse des OSE ou des OIV, néanmoins, **aucune disposition législative ou réglementaire ne détermine avec précision ni les prérogatives reconnues aux agents chargés du contrôle** de la sécurité des systèmes d'information dans le cadre de celui-ci, **ni les obligations qui s'imposent à eux.**

B. Le Gouvernement souhaite déterminer les droits et obligations des agents chargés du contrôle et des personnes contrôlées

Le présent article vise à **obliger les personnes faisant l'objet d'un contrôle de l'Anssi à mettre à disposition des agents ou personnels chargés du contrôle les moyens nécessaires pour effectuer les vérifications** sur pièces et sur place et **évaluer leur conformité aux exigences et le respect des obligations qui leur incombent**.

---

[1] *Article R. 1332-41-13 du code de la défense.*
[2] *Article R. 1332-41-14 du code de la défense.*
[3] *Article R. 1332-41-15 du code de la défense.*

Le **droit d'accès de ces agents et personnels aux locaux des entités contrôlées** serait consacré, étant précisé qu'ils peuvent pénétrer dans les lieux à usage professionnel.

Au surplus, ceux-ci seraient habilités à :

- **exiger la communication de tout document nécessaire à l'accomplissement de leur mission**, quel qu'en soit le support, et à obtenir ou prendre copie de ces documents par tout moyen et sur tout support, y compris les éléments de nature à établir la mise en œuvre effective par l'entité contrôlée des mesures de nature à répondre à ses obligations, dont les rapports d'audit menés par des organismes indépendants ;

- recueillir, sur place ou sur demande, **tout renseignement ou toute justification utile** ;

- **accéder aux systèmes d'information, aux logiciels, aux programmes informatiques et aux données stockées** et en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins de la supervision ;

- **procéder, sur convocation ou sur place, aux auditions de toute personne** susceptible d'apporter des éléments utiles à leurs constatations – le cas échéant, ils en dresseraient procès-verbal, que les personnes entendues liraient et signeraient tout en pouvant y faire consigner leurs observations ; en cas de refus de signer, mention en serait faite sur le procès-verbal.

Il est prévu que le secret professionnel ne puisse être opposé par les personnes contrôlées aux agents ou personnels chargés du contrôle agissant dans le cadre de leurs pouvoirs de contrôle.

Dans le même temps, ces agents et personnels ainsi que les experts qui concourront à l'accomplissement de leur mission de recherche et de constatation des manquements à la réglementation et des infractions en matière de cybersécurité seraient **astreints au secret professionnel pour les faits, actes ou renseignements dont ils auraient connaissance en raison de leurs fonctions**, sous réserve des éléments utiles à l'établissement des documents nécessaires à l'instruction.

Les rapports, avis ou autres documents justifiant d'adopter les mesures mentionnées aux articles 28, 29 et 32 du présent projet de loi – c'est-à-dire, respectivement, l'application d'une amende administrative en cas d'obstacle au contrôle, la mise à la charge de la personne contrôlée du coût du contrôle et la mise en œuvre d'une mesure d'exécution –, y compris ceux établis ou recueillis dans le cadre de la recherche de manquement, pourraient être **communiquées à la personne contrôlée**.

Enfin, il serait dressé procès-verbal des vérifications et visites menées dans le cadre du contrôle, qui ferait foi jusqu'à preuve du contraire.

II. La position de la commission : des modifications rédactionnelles et une sécurisation juridique

La commission se félicite que soient enfin déterminées avec précision les prérogatives et obligations des agents et personnels chargés des contrôles menés par l'Anssi, qui n'étaient jusqu'alors fixées par aucun texte de nature législative ou réglementaire.

Elle a par conséquent adopté le présent article assorti d'**un amendement n° COM-110** des rapporteurs y apportant des modifications de nature rédactionnelle et tendant à **en renforcer la sécurité juridique**, notamment en ce qui concerne les **modalités d'établissement des procès-verbaux d'auditions**.

La commission a adopté cet article ainsi modifié.

Article 28

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

Cet article vise à obliger la personne contrôlée à par l'Anssi à coopérer avec elle et à instaurer une amende administrative prononcée en cas d'obstacle au contrôle.

La commission a adopté un amendement procédant à des modifications rédactionnelles et de sécurisation juridique.

La commission a adopté cet article ainsi modifié.

I. Les modifications proposées par le Gouvernement : l'instauration d'un devoir de coopération de la personne contrôlée par l'Anssi et l'application d'une amende administrative en cas d'obstacle au contrôle

A. Le régime de sanctions pénales applicable en cas de manquement d'un opérateur à ses obligations, inadapté aux enjeux, n'est pas mis en œuvre

1. Des sanctions pénales sont prévues en cas d'obstacle à un contrôle de l'Anssi

S'**il n'existe pas de régime de sanction unique pour les faits d'obstacle à un contrôle** de l'Agence nationale de la sécurité des systèmes d'information (Anssi), une **amende de 125 000 €** est d'ores et déjà prévue **en cas d'obstacle de la part des dirigeants d'un opérateur de services essentiels** (OSE) aux opérations de contrôle du niveau de sécurité des systèmes d'information et du respect de leurs obligations en la matière[1].

En outre, **le fait, pour les dirigeants d'un opérateur d'importance vitale (OIV), de ne pas satisfaire à un certain nombre de leurs obligations**, et notamment à celle de soumettre les systèmes d'information de l'OIV à des contrôles destinés à vérifier leur niveau de sécurité et le respect des règles de sécurité nécessaires à leur protection, est **puni d'une amende de 150 000 €**[2].

2. Un régime d'amendes administratives doit être instauré en application de la directive NIS 2

L'article 34 de la directive dite « NIS 2 »[3] instaure **un régime d'amendes administratives en cas de non-respect des obligations qu'elle instaure**, ce qui facilitera la mise en œuvre effective des pénalités financières

---

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 9.*

[2] *Article L. 1332-7 du code de la défense.*

[3] *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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).*

dans un contexte de fort accroissement du nombre d'entités contrôlées par l'Anssi.

L'étude d'impact du présent projet de loi précise d'ailleurs que le régime de sanctions pénales actuellement en vigueur en France n'a **jamais été mis en œuvre**, dans la mesure où il n'offre pas à l'Anssi la possibilité d'une approche graduée.

Aussi est-il prévu que les États membres veillent à ce que, lorsqu'elles violent leurs obligations en matière de gestion des risques cyber et d'information, les entités importantes soient soumises à des amendes administratives d'un montant maximal s'élevant **au moins à 7 millions d'euros ou à 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle appartient l'entité concernée**, le montant le plus élevé étant retenu.

S'agissant des entités essentielles, ces seuils planchers sont **portés à 10 millions d'euros et à 2 % du chiffre d'affaires**.

La directive permet en outre à chaque État membre d'établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des entités de l'administration publique.

B. Le Gouvernement propose d'instaurer un devoir de coopération de la personne contrôlée par l'Anssi et de punir d'une amende administrative le fait de faire obstacle au contrôle

Le présent article tend à **obliger la personne contrôlée à coopérer avec l'Anssi**. Il habilite dans le même temps les agents et personnels chargés du contrôle à **constater toute action de la part de la personne contrôlée de nature à faire obstacle au contrôle**.

Le fait, pour la personne contrôlée, de faire obstacle aux demandes de l'Anssi nécessaires à la recherche des manquements et à la mise en œuvre de ses pouvoirs de contrôle, notamment en fournissant des renseignements incomplets ou inexacts ou en communiquant des pièces incomplètes ou dénaturées, serait constitutif d'un manquement et **puni d'une amende administrative prononcée par la commission des sanctions** instituée par l'article 1er du présent projet de loi.

Le montant de cette amende, **proportionné à la gravité du manquement**, ne pourrait excéder **10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial**, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu – **soit le plafond minimal fixé par la directive dite « NIS 2 »** pour les amendes administratives prononcées à l'encontre des entités essentielles.

Les griefs constitutifs d'obstacle au contrôle retenus à l'encontre de la personne contrôlée lui seraient notifiés par l'Anssi, laquelle saisirait la commission des sanctions afin qu'elle se prononce.

Il est enfin précisé que **ces dispositions ne s'appliqueraient ni aux administrations de l'État, ni à ses établissements publics administratifs**. Le Conseil d'État justifie cette exclusion au motif que « *le Gouvernement dispose à leur égard d'autres moyens que ces amendes pour garantir le respect de leurs obligations* »[1]. Les collectivités territoriales et leurs groupements et établissement seraient, pour leur part, soumises à ces dispositions du fait de « *l'absence de dispositif équivalent* » qui leur soit applicable.

II. La position de la commission : des modifications rédactionnelles et de sécurisation juridique

Dans la mesure où le champ des entités soumises aux contrôles de l'Anssi fait l'objet d'une extension dans le cadre de la transposition de la directive dite « NIS 2 », il est logique que soit instauré **un régime de sanction unique pour ce qui concerne les faits d'obstacle à un contrôle**.

Considérant qu'il se borne à transposer les dispositions de ladite directive en fixant le montant plafond des amendes administratives pouvant être prononcées dans ce cas au niveau minimal prévu par celle-ci, la commission a adopté le présent article assorti d'**un amendement n° COM-111** des rapporteurs y apportant des modifications de nature rédactionnelle et précisant que le chiffre d'affaires retenu pour la détermination du plafond de l'amende est **celui de l'entreprise à laquelle appartient la personne contrôlée**, conformément aux prescriptions de la directive.

La commission a adopté cet article ainsi modifié.

[1] *Conseil d'État, avis sur un projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier, séance du 6 juin 2024.*

Article 29
Forme et prise en charge financière des contrôles

Cet article vise à prévoir les formes que pourraient revêtir les contrôles de l'Anssi et à en faire supporter le coût par la personne contrôlée.

La commission a adopté un amendement de clarification juridique relatif à la prise en charge du coût des contrôles de l'Anssi.

La commission a adopté cet article ainsi modifié.

I. Les modifications proposées par le Gouvernement : la fixation des formes possibles des contrôles de l'Anssi et leur financement par la personne contrôlée

A. La réglementation prévoit d'ores et déjà la prise en charge du coût des contrôles par les opérateurs, mais pas la forme qu'ils peuvent revêtir

1. La forme des contrôles de l'Anssi, dont le coût est pris en charge par les opérateurs contrôlés, n'est pas suffisamment encadrée

Aucune disposition législative ou réglementaire ne détermine pour l'heure **la forme que peut revêtir un contrôle de l'Agence nationale de la sécurité des systèmes d'information (Anssi)**.

En tout état de cause, **la loi met le coût du contrôle à la charge de la personne contrôlée** dans le cas des contrôles destinés à vérifier le niveau de sécurité des systèmes d'information des opérateurs de services essentiels (OSE) et des opérateurs d'importance vitale (OIV) et le respect des règles de sécurité en la matière[1].

S'agissant des OIV, la réglementation en vigueur précise que, lorsqu'un contrôle est effectué par un service de l'État, son coût est calculé **en fonction du temps nécessaire à la réalisation du contrôle et du nombre d'agents publics qui y participent**, un arrêté du Premier ministre fixant le coût d'un contrôle mobilisant un agent public pendant une journée[2]. Dans le cas d'un contrôle effectué par un prestataire de service, le coût du contrôle est déterminé **librement par les parties**.

2. La directive NIS 2 liste différents types de contrôles auxquels les entités essentielles et importantes doivent pouvoir être soumises et prévoit la prise en charge par l'entité du coût des audits ciblés réalisés par un organisme indépendant

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 8 ; article L. 1332-6-3 du code de la défense.*
[2] *Article R. 1332-41-17 du code de la défense.*

Aux termes des articles 32 et 33 de la directive dite « NIS 2 »[1], les États membres doivent veiller à ce que les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités essentielles ou importantes, aient le pouvoir de soumettre ces entités, *a minima*, à :

- **des inspections sur place et des contrôles à distance**, y compris des contrôles aléatoires effectués par des professionnels formés ;

- **des audits de sécurité réguliers et ciblés** réalisés par un organisme indépendant ou une autorité compétente ;

- **des scans de sécurité** fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée ;

- **des demandes d'informations** nécessaires à l'évaluation – *ex post* dans le cas des entités importantes – des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27 de la directive ;

- **des demandes d'accès à des données, à des documents et à toutes informations nécessaires** à l'accomplissement de leurs tâches de supervision ;

- **des demandes de preuves de la mise en œuvre des politiques de cybersécurité**, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Au surplus, les entités essentielles doivent pouvoir être soumises à des audits *ad hoc*, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation de la directive par l'entité.

Il est précisé que le coût d'un audit de sécurité ciblé effectué par un organisme indépendant doit être **supporté par l'entité contrôlée**, **sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés**.

B. Le Gouvernement propose de déterminer les formes possibles d'un contrôle de l'Anssi et d'en mettre le coût à la charge de la personne contrôlée

Le présent article tend à li**ster les différentes formes que pourrait prendre un contrôle de l'Anssi**, à savoir :

- des inspections sur place et des contrôles à distance ;

- des audits de sécurité réguliers et ciblés réalisés par l'Anssi ou par un organisme indépendant choisi par elle ;

- des scans de sécurité ;

---

[1] *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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).*

- et des audits en cas d'incident important ou d'une violation des dispositions de l'article 26 du présent projet de loi, qui habilite les agents de l'Anssi ainsi que des organismes indépendants et des services de l'État spécialement désignés à cet effet à rechercher et constater les manquements à la réglementation et les infractions en matière de cybersécurité.

Il est par ailleurs prévu que le coût du contrôle soit **supporté par la personne contrôlée, sauf si, à titre exceptionnel, l'Anssi en décidait autrement**. D'après l'étude du présent projet de loi, ce choix découlerait de la volonté d'appliquer « *un principe de redevance pour service rendu, conformément à la jurisprudence du Conseil d'État* », et ce « *dans un souci d'harmonisation* » avec les dispositifs actuellement applicables aux OIV et aux OSE.

Du reste, et pour mémoire, l'article 27 du présent projet de loi habilite notamment les agents ou personnes chargés des contrôles à exiger la communication de tout document nécessaire à l'accomplissement de leur mission, quel qu'en soit le support, et à obtenir ou prendre copie de ces documents par tout moyen et sur tout support, y compris les éléments de nature à établir la mise en œuvre effective par l'entité contrôlée des mesures de nature à répondre à ses obligations, dont les rapports d'audit menés par des organismes indépendants.

II. La position de la commission : une clarification juridique relative à la prise en charge du coût des contrôles de l'Anssi

La commission constate que le présent article se borne à transposer en droit national les dispositions de la directive déterminant la forme que peuvent revêtir les contrôles de l'Anssi.

En revanche, le choix de faire reposer le coût de ces contrôles sur la personne contrôlée va bien **au-delà des prescriptions de la directive –** laquelle ne met à la charge des entités contrôlées que le coût des audits de sécurité ciblés effectués par un organisme indépendant, sauf décision contraire de l'autorité compétente.

D'après les informations recueillies au cours des auditions menées par les rapporteurs, il pourrait être envisagé de ne faire supporter le coût d'un contrôle par la personne faisant l'objet de ce contrôle **que dans le cas où celui-ci révèlerait une infraction ou un manquement aux obligations qui s'imposent à la personne contrôlée**.

En tout état de cause, l'ensemble des parties prenantes entendues par la commission spéciale – entreprises comme collectivités territoriales – se sont élevées contre le principe même de faire reposer le coût des contrôles, sans distinction ni précision particulière, sur la personnes contrôlée, l'exonération exceptionnelle que pourrait accorder l'Anssi apparaissant purement discrétionnaire.

Par conséquent, sur la proposition des rapporteurs, la commission a adopté **un amendement de clarification juridique n° COM-112** visant à préciser explicitement que la personne contrôlée n'est pas tenue de prendre en charge le coût du contrôle lorsque celui-ci ne révèle aucune infraction ou manquement auxdites obligations.

La commission a adopté cet article ainsi modifié.

Article 30

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

Cet article vise à renvoyer à un décret en Conseil d'État la détermination des modalités d'application des dispositions relatives aux prérogatives de l'Anssi en matière de recherche et de constatation des manquements.

La commission a adopté cet article sans modification.

I. Les modifications proposées par le Gouvernement : la fixation des modalités d'application par décret en Conseil d'État

Le présent article tend à prévoir la fixation des modalités d'application de la sous-section 2 de la section 1 du chapitre III du présent projet de loi, qui détermine les prérogatives de l'Anssi en matière de recherche et de constatation des manquements, par **un décret en Conseil d'État**.

II. La position de la commission : une adoption sans modification

Les dispositions proposées n'appellent pas de commentaire de la part de la commission, qui se déclare favorable à son adoption.

La commission a adopté cet article sans modification.

SECTION 2
MESURES CONSÉCUTIVES AUX CONTRÔLES

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

Cet article vise à permettre à l'Anssi d'ouvrir une procédure à l'encontre de la personne contrôlée au vu des résultats du contrôle.

La commission a adopté un amendement de sécurisation et de clarification juridiques en intégrant à cet article les dispositions de l'article 32, en précisant les modalités d'ouverture d'une procédure et en supprimant les dispositions permettant à l'Anssi de rendre publique la mesure d'exécution adoptée et d'enjoindre à la personne contrôlée de rendre public son manquement.

La commission a adopté cet article ainsi modifié.

I. Les modifications proposées par le Gouvernement : l'ouverture par l'Anssi d'une procédure à l'issue d'un contrôle

A. Les dirigeants des opérateurs ne se conformant pas à leurs obligations en matière de sécurité des systèmes d'information après avoir été mis en demeure de le faire sont passibles d'une amende

Lorsqu'un manquement est constaté dans le cadre d'un contrôle du niveau de sécurité des réseaux et systèmes d'information d'un opérateur de services essentiels (OSE) et du respect des règles de sécurité en la matière, l'Anssi peut **mettre en demeure les dirigeants de l'OSE concerné de se conformer**, dans un délai qu'elle détermine en tenant compte des conditions de fonctionnement de l'OSE et des mesures à mettre en œuvre, **aux obligations qui leur incombent**[1].

Le fait, pour les dirigeants d'un OSE, de ne pas se conformer aux règles de sécurité qui s'imposent à eux à l'issue du délai fixé par la mise en demeure est puni de **100 000 € d'amende**[2].

De même, **le fait, pour les dirigeants d'un opérateur d'importance vitale (OIV), de ne pas satisfaire à leurs obligations en matière de sécurité des réseaux et systèmes d'information est puni d'une amende de 150 000 €**, cette sanction étant précédée d'une mise en demeure[3].

B. Le Gouvernement entend permettre l'ouverture par l'Anssi d'une procédure au terme d'un contrôle

---

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 8.*
[2] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, article 9.*
[3] *Article L. 1332-7 du code de la défense.*

Le présent article tend à permettre à l'Anssi d'engager **une procédure à l'encontre de la personne contrôlée au vu des résultats d'un contrôle**.

L'Anssi devrait dès lors notifier sa décision à la personne contrôlée et désigner parmi les agents et personnes habilités un ou plusieurs rapporteurs chargés de l'instruction de cette procédure.

II. La position de la commission : des modifications de sécurisation et de clarification juridiques

La commission juge nécessaire de permettre le déclenchement d'une procédure à l'encontre de la personne contrôlée **lorsque le contrôle révèle un manquement aux obligations qui s'imposent à la personne contrôlée**. Elle a par conséquent adopté un **amendement n° COM-113** des rapporteurs prévoyant explicitement l'ouverture d'une procédure de cette nature dans un tel cas.

Par ailleurs, dans un souci de **clarification de l'objectif poursuivi lors de l'ouverture par l'Anssi d'une telle procédure**, cet amendement tend également à **intégrer au présent article les dispositions de l'article 32** du présent projet de loi, qui permettent à l'Anssi soit de clore la procédure lorsque les faits constatés ne justifient pas l'adoption d'une mesure d'exécution, soit d'adopter une telle mesure si celle-ci s'avère nécessaire pour mettre un terme à l'infraction ou au manquement.

Enfin, il supprime la faculté accordée à l'Anssi de rendre publique la mesure d'exécution adoptée et d'enjoindre à la personne contrôlée de rendre public son manquement. Seule la commission des sanctions serait donc habilitée à décider d'une mesure de publicisation, dans la mesure où celle-ci constitue davantage une sanction qu'une mesure de police administrative.

La commission a adopté cet article ainsi modifié.

Article 32
Mesures d'exécution

Cet article vise à déterminer la manière dont pourrait se poursuivre la procédure ouverte par l'Anssi à l'encontre de la personne contrôlée, et notamment les mesures d'exécution pouvant être mises en œuvre.

La commission a adopté un amendement de suppression de cet article.

I. Les modifications proposées par le Gouvernement : la possibilité pour l'Anssi de mettre en œuvre des mesures d'exécution au terme de la procédure initiée à l'issue d'un contrôle

A. La directive NIS 2 impose aux États membres de permettre l'adoption de mesures d'exécution à l'encontre des entités contrôlées

Les articles 32 et 33 de la directive dite « NIS 2 »[1] prévoient que les États membres veillent à ce que leurs autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles ou importantes, aient *a minima* le pouvoir :

- **d'émettre des avertissements** concernant les violations de la directive par les entités concernées ;

- **d'adopter des instructions contraignantes**, y compris en ce qui concerne les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre, ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la directive ;

- **d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la directive** et de ne pas le réitérer ;

- d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 21 de la directive ou de respecter les obligations d'information prévues par son article 23, de manière spécifique et dans un délai déterminé ;

- **d'ordonner aux entités concernées d'informer les personnes physiques ou morales** à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante **de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace** ;

[1] *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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).*

- **d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées** à la suite d'un audit de sécurité dans un délai raisonnable ;

- **d'ordonner aux entités concernées de rendre publics les aspects de violations de la directive** de manière spécifique ;

- et **d'imposer ou de demander aux organes compétents ou aux juridictions d'imposer, conformément au droit national, une amende administrative** en plus d'une mesure d'exécution.

S'agissant spécifiquement des entités essentielles, les autorités compétentes doivent également pouvoir désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des articles 21 et 23 de la directive.

En outre, lorsque les mesures d'exécution adoptées sont inefficaces, les États membres doivent veiller à ce que leurs autorités compétentes aient le pouvoir **de fixer un délai dans lequel l'entité essentielle soit invitée à prendre les mesures nécessaires** pour pallier les insuffisances ou satisfaire aux exigences de ces autorités.

Si la mesure demandée n'est pas prise dans le délai imparti, les États membres doivent veiller à ce que les autorités compétentes aient le pouvoir **de suspendre temporairement** ou de demander à un organisme de certification ou d'autorisation ou à une juridiction, conformément au droit national, de suspendre temporairement **une certification ou une autorisation** concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité essentielle.

Au surplus, aux termes de l'article 34 de la directive, les États membres peuvent prévoir le pouvoir **d'imposer des astreintes** pour contraindre une entité essentielle ou importante à mettre un terme à une violation de la directive conformément à une décision préalable de l'autorité compétente.

B. Le Gouvernement entend permettre à l'Anssi soit de clore la procédure ouverte à l'issue d'un contrôle, soit d'adopter une mesure d'exécution

Le présent article tend à déterminer la manière dont pourrait se poursuivre la procédure ouverte par l'Anssi à l'encontre de la personne contrôlée au vu des résultats d'un contrôle.

Dans le cas où l'instruction ne ferait pas état de faits justifiant une mesure d'exécution, **l'Anssi clôturerait la procédure** et en informerait la personne concernée.

En revanche, dans le cas contraire, **l'Anssi serait habilitée à adopter une mesure d'exécution** après avoir mis la personne concernée en mesure de présenter ses observations. Elle pourrait ainsi :

- prononcer une mise en garde à l'encontre de la personne contrôlée ;

- lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier et définir les délais accordés pour les mettre en œuvre et en rendre compte ;

- lui enjoindre de se mettre en conformité avec les obligations qui lui sont applicables dans un délai qu'elle détermine et qui ne peut être inférieur à un mois, sauf en cas de manquement gravé ou répété ;

- lui ordonner d'informer les personnes physiques ou morales au profit desquelles elle fournit des services ou exerce des activités susceptibles d'être affectées par une cybermenace importante de la nature de cette menace et de toute mesure préventive ou réparatrice qu'elles pourraient prendre pour répondre à cette menace ;

- lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ;

- et exiger qu'elle informe le public du manquement constaté par tout moyen adapté.

Le cas échéant, la mesure d'exécution devrait être **notifiée aux intéressés** et pourrait être **assortie d'une astreinte dont le montant serait plafonné à 5 000 euros par jour de retard**. L'Anssi serait autorisée à **rendre cette mesure publique**.

Il est enfin précisé que l'astreinte journalière courrait à compter du jour suivant l'expiration du délai imparti aux personnes concernées pour déférer à l'injonction. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions instituée par l'article 1er du présent projet de loi pourrait procéder à la liquidation de cette astreinte.

II. La position de la commission : la suppression de cet article

Les dispositions du présent article, qui n'appellent pas de modification de fond – dans la mesure où elles se bornent à transposer les dispositions de la directive dite « NIS 2 » –, mais uniquement des modifications de nature rédactionnelle, ont été **intégrées à l'article 31** du présent projet de loi par **un amendement n° COM-113** des rapporteurs, dans un souci de **clarification de l'objectif poursuivi lors de l'ouverture par l'Anssi d'une procédure** à l'encontre de la personne contrôlée.

Par conséquent, la commission a adopté **un amendement n° COM-114** des rapporteurs visant à **supprimer le présent article**.

La commission a supprimé cet article.

Article 33
Saisine de la commission des sanctions

Cet article vise à prévoir la saisine par l'Anssi de la commission des sanctions en cas d'inexécution d'une mesure d'exécution.

La commission a adopté un amendement rédactionnel et de coordination.

La commission a adopté cet article ainsi modifié.

I. Les modifications proposées par le Gouvernement : la saisine de la commission des sanctions en cas d'inexécution d'une mesure d'exécution

Le présent article tend à déterminer la manière dont pourrait se conclure la procédure ouverte par l'Anssi à l'encontre de la personne contrôlée dans le cas où il aurait été décidé d'une mesure d'exécution.

Il prévoit que **l'Anssi constate qu'il n'y a pas lieu de poursuivre la procédure** et notifie sa décision à la personne concernée **lorsque celle-ci fournit des éléments montrant qu'elle s'est conformée à la mesure d'exécution dans le délai imparti**.

En revanche, dans le cas où la personne concernée ne se serait pas conformée à l'une des mesures d'exécution prononcées par l'Anssi, cette dernière lui notifierait les griefs retenus et **saisirait la commission des sanctions** instituée par l'article 1er du présent projet de loi.

Du reste, dans l'hypothèse où la personne concernée serait une entité essentielle et où elle n'apporterait pas la preuve qu'elle s'est conformée, dans le délai imparti, à quatre types de mesures d'exécution – mise en garde, injonction de prendre les mesures nécessaires pour éviter un incident ou y remédier, injonction de se mettre en conformité avec les obligations applicables et injonction de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité –, l'Anssi serait autorisée à **suspendre une certification ou une autorisation concernant tout ou partie des services fournis ou des activités exercées par cette entité jusqu'à ce que celle-ci ait remédié au manquement**.

Si cette certification ou cette autorisation a été délivrée par un organisme de certification ou d'autorisation, il est prévu que l'Anssi enjoigne à cet organisme de la suspendre jusqu'à ce que l'entité ait remédié au manquement.

II. La position de la commission : des modifications rédactionnelles et de coordination

Le présent article se bornant, comme les précédents, à transposer les dispositions de la directive dite « NIS 2 » visant à mettre un terme aux

infractions et aux manquements aux obligations incombant aux personnes contrôlées et s'inscrivant dans le cadre du régime de sanctions administratives institué par ladite directive, la commission n'a identifié aucun obstacle à son adoption.

Elle a néanmoins adopté **un amendement n° COM-115** des rapporteurs visant à améliorer la qualité rédactionnelle du dispositif, à procéder aux coordinations découlant de l'intégration des dispositions de l'article 32 du présent projet de loi à l'article 31 et à **exclure les avertissements du champ des mesures d'exécution dont la non-application peut entraîner la suspension d'une certification ou d'une autorisation** par l'Anssi, compte tenu du fait qu'il n'est pas possible, à proprement parler, de se conformer à un avertissement, dont le prononcé n'appelle pas la mise en œuvre d'une action, mais plutôt la non-réitération d'un fait.

La commission a adopté cet article ainsi modifié.

Article 34

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

Cet article vise à renvoyer à un décret en Conseil d'État la détermination des modalités d'application des dispositions relatives à la procédure pouvant être engagée par l'Anssi à l'encontre de la personne contrôlée.

La commission a adopté cet article sans modification.

I. Les modifications proposées par le Gouvernement : la fixation des modalités de la procédure pouvant être ouverte à l'encontre de la personne contrôlée par décret en Conseil d'État

Le présent article tend à prévoir la fixation par **un décret en Conseil d'État** des modalités d'application de la section 2 du chapitre III du présent projet de loi, qui détermine le cadre juridique applicable à la procédure pouvant être engagée par l'Anssi à l'encontre de la personne contrôlée au terme d'un contrôle.

II. La position de la commission : une adoption sans modification

Les dispositions proposées n'appellent pas de commentaire de la part de la commission, qui se déclare favorable à son adoption.

La commission a adopté cet article sans modification.

Article 35
Compétence de la commission des sanctions

Cet article prévoit que la commission des sanctions en matière de cybersécurité placée auprès du Premier ministre prévue à l'article L. 1332-15 du code de la défense est compétente pour statuer sur l'application des chapitre II « De la cyber résilience » et III « De la supervision » du présent projet de loi

La commission a adopté cet article sans modification.

I. La situation actuelle – la création d'une commission des sanctions en matière de cybersécurité constitue une nouveauté

Il n'existe pour l'heure **pas de commission des sanctions en matière de cybersécurité**, celle-ci constituant **une innovation** du présent projet de loi qui vise à garantir **la bonne application** des mesures qu'il prévoit pour que **l'ensemble des entités concernés élèvent leur niveau de cybersécurité**.

Cette innovation résulte directement des dispositions de l'article 36 de la directive NIS 2 qui prévoit que les États membres déterminent **le régime des sanctions applicables** aux violations des dispositions nationales adoptées conformément à la directive et prennent **toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions**.

L'article 36 précise que **les sanctions** prévues doivent être **effectives**, **proportionnées** et **dissuasives**.

II. Le dispositif envisagé – une même commission des sanctions pour les manquements prévus aux obligations prévues par les directives REC et NIS 2

L'article 1er du présent projet de loi introduit un article L. 1332-15 au code de la défense qui prévoit **la création d'une commission des sanctions instituée auprès du Premier ministre**.

L'article 35 prévoit que cette commission des sanctions statue sur les manquements constatés aux obligations découlant de l'application du chapitre II « De la cyber résilience », c'est-à-dire les articles 6 à 24, et du chapitre III « De la supervision », c'est-à-dire les articles 25 à 37, dans les conditions prévues par la présente section « Des sanctions » qui comprend les articles 35 à 37.

Cette commission est saisie **par l'autorité administrative des manquements constatés**. L'autorité, en l'occurrence l'Anssi, notifie à l'opérateur concerné **les griefs susceptibles d'être retenus à son encontre**.

La commission des sanctions **reçoit les rapports et procès-verbaux des contrôles réalisés par l'autorité**.

III. La position de la commission – une commission commune des sanctions mais avec une composition adaptée

Le présent article, qui prévoit que la commission des sanctions créé au titre I du projet de loi est compétente pour statuer sur les manquements constatés aux obligations découlant de l'application des chapitres II et III du titre II, ne présente pas de difficultés, dans la mesure où l'article 36 prévoit **une composition adaptée avec la nomination de personnalités qualifiées compétentes dans le domaine de la sécurité des systèmes d'information**.

La commission a adopté cet article sans modification.

Article 36
Composition de la commission des sanctions

Cet article prévoit la composition de la commission des sanctions en matière de cybersécurité placée auprès du Premier ministre, lorsqu'elle doit statuer sur l'application des chapitre II « De la cyber résilience » et III « De la supervision » du présent projet de loi.

La commission a adopté trois amendements visant à :

- prévoir une nomination des trois personnalités qualifiées en raison de leur expertise en matière de sécurité par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat, et non par le seul Premier ministre ;

- s'assurer que ces personnes qualifiées n'auront pas travaillé au sein de l'Anssi depuis moins de cinq ans ;

- préciser que c'est l'Anssi qui saisit la commission des sanctions.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle – la mise en place d'une commission des sanctions qui découle de la transposition de la directive NIS 2

Il n'existe pour l'heure **pas de commission des sanctions en matière de cybersécurité**, celle-ci constituant une innovation qui vise à **garantir la bonne application des mesures** prévues par le projet de loi pour que l'ensemble des entités concernées **élèvent leur niveau de cybersécurité**. Cette commission des sanctions est introduite aux articles L. 1332-15 et suivants du code de la défense par l'article 1er du présent projet de loi.

Comme indiqué dans le commentaire de l'article 35, cette innovation résulte directement **des dispositions de l'article 36 de la directive NIS 2** qui prévoit que les États membres déterminent **le régime des sanctions applicables** aux violations des dispositions nationales adoptées conformément à la directive et prennent **toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions**.

L'article 36 de la directive NIS 2 précise que **les sanctions** prévues doivent être **effectives**, **proportionnées** et **dissuasives**.

II. Le dispositif envisagé – les trois personnalités qualifiées membres de la commission des sanctions lorsqu'elle est compétente en matière de cybersécurité seraient toutes nommées par le Premier ministre

L'article 36 du projet de loi prévoit que lorsqu'elle est saisie **de manquements aux obligations** découlant de l'application du chapitre II « De la cyber résilience » et du chapitre III « De la supervision » du présent projet de loi, **la commission des sanctions en matière de cybersécurité** prévue aux

articles L. 1332-15 et suivants du code de la défense et **placée auprès du Premier ministre** est composée :

- **des personnes** mentionnées au 1° de l'article L. 1332-16 du code de la défense, c'est-à-dire **d'un membre du Conseil d'État**, **président**, désigné par le vice-président du Conseil d'État, **d'un membre de la Cour de cassation** désigné par le premier président de la Cour de cassation et **d'un membre de la Cour des comptes** désigné par le premier président de la Cour des comptes ;
- **de trois personnalités qualifiées**, **nommés par le Premier ministre** en raison de **leurs compétences dans le domaine de la sécurité des systèmes d'information**.

L'article L. 1332-16 du code de la défense, tel que prévu par l'article 1er du présent projet de loi, prévoit que **les membres de la commission des sanctions exercent leurs fonctions en toute impartialité**. Dans l'exercice de leurs attributions, ils **ne reçoivent ni ne sollicitent d'instruction d'aucune autorité**.

Le président de la commission, qui est un membre du Conseil d'État, désigne **un rapporteur parmi ses membres**. Celui-ci **ne peut recevoir aucune instruction**.

La commission des sanctions **statue par décision motivée**. Aucune sanction **ne peut être prononcée sans que l'opérateur concerné ou son représentant ait été entendu** ou, à défaut, dûment convoqué. La commission peut **auditionner toute personne qu'elle juge utile**.

La commission statue **à la majorité des membres présents**. En cas de partage égal des voix, celle du président est prépondérante.

Le président et les membres de la commission ainsi que leurs suppléants respectifs sont **nommés par décret pour un mandat de cinq ans**, **renouvelable une fois**. Ils sont tenus **au secret professionnel**.

III. La position de la commission – un ajustement des autorités de nomination des personnalités qualifiées pour renforcer l'indépendance de la commission des sanctions

Si elle n'a **pas remis en cause la composition de la commission des sanctions** proposée à l'article 36, la commission spéciale a adopté, outre un amendement COM 117 du rapporteur Patrick Chaize précisant que **c'est l'autorité nationale de sécurité des systèmes d'information qui saisit la commission des sanctions** :

- un amendement COM 118 du rapporteur Patrick Chaize qui prévoit, pour renforcer les garanties d'indépendance de la

commission des sanctions, que **les trois personnalités qualifiées** en raison de leurs compétences dans le domaine de la sécurité des systèmes d'information qui y siègeront ne seront **pas uniquement désignées par le Premier ministre** mais nommées respectivement **par le Premier ministre**, **le président de l'Assemblée nationale** et **le président du Sénat** ;

- un amendement COM 119 du rapporteur Patrick Chaize qui prévoit, toujours afin de garantir au maximum l'indépendance de la commission des sanctions, que **les personnalités qualifiées** nommées dans son collège n'exercent **pas de responsabilités**, ou **n'ont pas exercé de responsabilités depuis moins de cinq ans**, au sein de **l'autorité nationale de sécurité des systèmes d'information**.

La commission a adopté l'article ainsi modifié.

Article 37

Sanctions en cas de manquements aux obligations en matière de cybersécurité

Cet article vise à transposer les différentes sanctions administratives prévues par la directive NIS 2 en cas de méconnaissance des obligations qu'elle impose aux entités régulées.

La commission a adopté deux amendements tendant à :

- prévoir que la faculté pour la commission des sanctions d'interdire à une personne physique exerçant les fonctions de dirigeant dans une entité « essentielle » qui n'aurait pas accompli toutes ses obligations en matière de cybersécurité d'exercer des responsabilités dirigeantes dans cette entité est possible uniquement en dernier recours, si et seulement si le manquement persiste alors que l'entité « essentielle » s'est déjà vue imposer une amende administrative ;

- prévoir que la sanction peut être rendue publique.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle – un dispositif de sanctions administratives prévu par la directive NIS 2 afin de garantir sa bonne application par les entités régulées

L'article 36 de la directive NIS 2 prévoit que les États membres déterminent **le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la directive** et prennent **toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions**.

L'article 36 précise que **les sanctions** prévues doivent être **effectives**, **proportionnées** et **dissuasives**.

Dans le même temps, l'article 34 de la directive intitulé « **Conditions générales pour imposer des amendes administratives à des entités essentielles et importantes** » prévoit lui aussi que les États membres veillent à ce que **les amendes administratives** imposées aux entités « essentielles » et « importantes » sur son fondement pour des violations de la directive soient **effectives**, **proportionnées** et **dissuasives**, compte tenu **des circonstances** de chaque cas.

Le paragraphe 4 de l'article 34 prévoit que les États membres veillent à ce que, lorsqu'elles violent l'article 21 (article sur **les mesures de gestion des risques en matière de cybersécurité** transposé par l'article 14 du présent projet de loi) ou 23 (article sur **les obligations de notification et d'information** transposé par l'article 17 du présent projet de loi), les entités « essentielles » soient soumises à **des amendes administratives d'un montant maximal** s'élevant à au **moins 10 millions d'euros** ou à **au moins 2 % du**

chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité « essentielle » appartient, le montant le plus élevé étant retenu.

Le paragraphe 5 de l'article 34 prévoit que les États membres veillent à ce que, lorsqu'elles violent l'article 21 (article sur **les mesures de gestion des risques en matière de sécurité** transposé par l'article 14 du présent projet de loi) ou 23 (article sur **les obligations d'information** transposé par l'article 17 du présent projet de loi), les entités « importantes » soient soumises **à des amendes administratives d'un montant maximal s'élevant à au moins 7 millions d'euros** ou à **au moins 1,4 % du chiffre d'affaires annuel mondial total** de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

Le paragraphe 7 de l'article 34 dispose que chaque État membre peut établir les règles déterminant **si et dans quelle mesure des amendes administratives peuvent être imposées à des entités de l'administration publique**.

Le point b) du paragraphe 5 de l'article 32 de la directive prévoit enfin que lorsque **les mesures d'exécution** ordonnées à une entité essentielle en matière de cybersécurité ne sont **pas prises dans le délai imparti**, les États membres veillent à ce que leurs autorités compétentes aient le pouvoir de demander aux organes compétents ou aux juridictions compétentes, conformément au droit national, **d'interdire temporairement à tout personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal** dans l'entité « essentielle » **d'exercer des responsabilités dirigeantes dans cette entité**.

Cette interdiction temporaire est **uniquement appliquée jusqu'à ce que l'entité concernée prenne les mesures nécessaires pour remédier aux insuffisances** ou **se conformer aux exigences** de l'autorité compétente à l'origine de l'application de ces mesures d'exécution.

L'imposition de ces suspensions ou interdictions temporaires est soumise à **des garanties procédurales appropriées** conformément **aux principes généraux du droit de l'Union et à la Charte**, y compris **le droit à un recours effectif** et à **accéder à un tribunal impartial**, **la présomption d'innocence** et **les droits de la défense**.

II. Le dispositif envisagé – des sanctions qui assurent une transposition fidèle de la directive

Le I de l'article 37 établit **les sanctions** que peut prononcer **la commission des sanctions** mentionnée aux articles 35 et 36 en cas de manquement constaté **aux obligations** prévues par les dispositions prévues au présent titre II « Cybersécurité » visant à transposer la directive NIS 2.

A l'encontre des entités « essentielles » définies à l'article 8 et des opérateurs mentionnés à l'article L. 1332-2 du code de la défense, il prévoit

une amende administrative dont **le montant**, **proportionné à la gravité du manquement**, **ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial**, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité « essentielle » appartient, le montant le plus élevé étant retenu. **Les administrations de l'État** et **de ses établissements publics administratifs**, **des collectivités territoriales**, **de leurs groupements** et **de leurs établissements publics administratifs** ne peuvent se voir appliquer cette sanction.

Cette sanction constitue **une transposition fidèle** du paragraphe 4 de l'article 34 de la directive NIS 2, avec **l'utilisation de l'exemption pour les administrations publiques** rendue possible par le paragraphe 7 dudit article 34.

A l'encontre **des entités « importantes »** définies à l'article 9, il prévoit **une amende administrative** dont **le montant**, **proportionné à la gravité du manquement**, **ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total**, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu. Là encore, **les administrations de l'État** et **de ses établissements publics administratifs**, **des collectivités territoriales**, **de leurs groupements** et **de leurs établissements publics administratifs** ne peuvent se voir appliquer cette sanction.

Cette sanction constitue **une transposition fidèle** du paragraphe 5 de l'article 34 de la directive NIS 2, avec l'utilisation de **l'exemption pour les administrations publiques** rendue possible par le paragraphe 7 dudit article 34.

À l'encontre **des offices d'enregistrement** et **des bureaux d'enregistrement** mentionnés à l'article 18 du présent projet de loi, à l'exception de ceux relevant des articles L. 45 à L. 45-8 du code des postes et des communications électroniques lorsqu'il s'agit d'un manquement aux obligations prévues à la section 3 du chapitre II du présent projet de loi, il prévoit **une amende administrative** dont **le montant**, **proportionné à la gravité du manquement**, **ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total**, hors taxes, de l'exercice précédent. Cette amende **peut se cumuler avec l'amende prévue pour les entités « essentielles »** à l'encontre d'un office d'enregistrement en cas de manquement aux obligations applicables aux entités « essentielles ».

Le quatrième alinéa de l'article 37 prévoit que si les manquements relevés constituent également une violation du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, donnant lieu à un amende administrative prononcée par la Commission nationale de l'informatique et des libertés (Cnil) en vertu des articles 20 à 22-1 de la loi n° 78-17 du 6 janvier

1978 relative à l'informatique, aux fichiers et aux libertés, **la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative**.

Le II de l'article 37 prévoit que **la commission peut prononcer une amende administrative** dont **le montant**, **proportionné à la gravité du manquement**, **ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total**, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu, à l'encontre :

- **des fournisseurs de moyens d'identification électronique** relevant des schémas d'identification électronique notifiés par l'État, **des prestataires de services de confiance** établis sur le territoire français, **des fournisseurs de dispositifs de création de signature et de cachet électronique** qualifié qu'elle certifie et **des organismes d'évaluation de la conformité**, à l'exception des administrations de l'État et de leurs établissements publics à caractère administratif, en cas de manquement constaté aux dispositions du règlement (UE) n° 910/2014 du 23 juillet 2014
- **des organismes d'évaluation de la conformité** sauf si l'organisme d'évaluation de la conformité est l'autorité nationale de certification de cybersécurité, **des titulaires d'une déclaration de conformité aux exigences d'un schéma de certification européen**, **des titulaires d'un agrément**, **d'une qualification** ou **d'un certificat dans le domaine de la cybersécurité**, en cas de manquement constaté aux dispositions du règlement (UE) n° 2019/881 du 17 avril 2019 ou aux exigences applicables mentionnés au 4° et au 5° de l'article 26 du présent projet de loi.

Le III de l'article 37 prévoit que lorsque la commission des sanctions envisage de prononcer l'amende prévue à l'article 28 à l'encontre de la même personne, **le montant cumulé des sanctions ne peut excéder** le montant de l'amende prévue au I ou au II du présent article 37, c'est-à-dire **10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total**, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.

Pour mémoire, l'article 28 prévoit que le fait, pour une personne contrôlée de **faire obstacle aux demandes de l'autorité nationale de sécurité des systèmes d'information** nécessaires à **la recherche des manquements** et à **la mise en œuvre des pouvoirs de cette dernière**, notamment en fournissant des renseignements incomplets ou inexacts ou en communiquant des pièces incomplètes ou dénaturées, est constitutif **d'un manquement** et puni **d'une amende administrative** prononcée par **la commission des sanctions** mentionnée à l'article 35 dont le montant, proportionné à la gravité du manquement, **ne peut excéder dix millions d'euros** ou **2 % du chiffre d'affaires annuel mondial**, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.

Le IV de l'article 37 prévoit que **la commission des sanctions** peut également prononcer les mesures suivantes à l'encontre **des organismes d'évaluation de la conformité et des titulaires d'agréments**, **de qualifications** ou **de certificats en matière de cybersécurité**, au titre des dispositions du règlement (UE) n° 910/2014 du 23 juillet 2014, des dispositions du règlement (UE) 2019/881 du 17 avril 2019 ou des exigences de cybersécurité mentionnés au 5° de l'article 26 du présent projet de loi, à savoir :

- **l'abrogation d'un agrément**, **d'une qualification** ou **d'un certificat** ;
- **l'abrogation de l'autorisation**, **de l'agrément** ou **de l'habilitation** délivré à l'organisme d'évaluation de la conformité, lorsque **le manquement n'est pas corrigé dans le délai imparti** par l'autorité nationale de sécurité des systèmes d'information.

Le V de l'article 37 prévoit enfin que la commission des sanctions peut **interdire à toute personne physique exerçant les fonctions de dirigeant dans l'entité « essentielle » d'exercer des responsabilités dirigeantes dans cette entité**, jusqu'à ce que l'entité « essentielle » ait remédié au manquement.

Cette sanction est prévue pour assurer la transposition du point b) du paragraphe 5 de l'article 32 de la directive.

Il est précisé que ces dispositions **ne s'appliquent pas aux administrations**.

III. La position de la commission – un encadrement de la sanction interdisant l'exercice par une personne physique de fonctions de direction au sein d'une entité « essentielle »

Lors de son audition, le directeur général de l'Anssi a indiqué que, sur **la question des sanctions**, le texte s'inscrit avant tout dans **une logique d'accompagnement des entités vers une mise en conformité**, la définition des sanctions permettant de **matérialiser les conséquences attachées**, à terme, à **une non-conformité**.

Dans cet esprit, le projet de loi se contente en la matière de **transposer à l'identique les mesures de la directive NIS 2 en matière d'amendes administratives**, les taux d'amendes visés, **2 % du chiffre d'affaires pour les entités « essentielles »** et **1,4 % pour les entités « importantes »** étant **des seuils maximaux**.

Si la commission spéciale a considéré que **la transposition de ces sanctions pécuniaires était en effet fidèle**, elle a en revanche estimé que prévoir, **sans aucune forme d'encadrement** que la commission des sanctions peut **interdire à toute personne physique** exerçant les fonctions de dirigeant dans l'entité « essentielle » **d'exercer des responsabilités dirigeantes dans cette entité**, jusqu'à ce que l'entité « essentielle » ait remédié au manquement, paraissait **problématique**.

En conséquence, elle a adopté un amendement COM 120 du rapporteur Patrick Chaize qui prévoit que **la faculté pour la commission des sanctions d'interdire à une personne physique exerçant les fonctions de dirigeant dans une entité « essentielle »** qui n'aurait pas accompli toutes ses obligations en matière de **cybersécurité d'exercer des responsabilités dirigeantes** dans cette entité est possible **uniquement en dernier recours**, **si et seulement si le manquement persiste** alors que l'entité « essentielle » **s'est déjà vue imposer une amende administrative**.

Il s'agit de **réserver cette sanction à des cas graves et exceptionnels** qui verraient **un dirigeant persister à refuser de résoudre un manquement** alors même que **son entreprise aurait déjà été sanctionnée**.

La commission a également adopté un amendement COM 121 du rapporteur Patrick Chaize qui prévoit que lorsque la commission des sanctions prononce l'une des sanctions prévues aux I, II, III et IV de l'article 37, **elle peut exiger que l'entité concernée communique au public**, par tout moyen adapté et à ses frais, **le manquement constaté**. La commission des sanctions peut également décider, dans l'intérêt du public, **de rendre publique sa décision ou un extrait de celle-ci**, selon des modalités qu'elle précise.

Il s'agit là d'un amendement de cohérence avec celui porté à l'article 32 qui tend à **renforcer les garanties attachées à la publicisation de mesures d'exécution qui pourrait être reconnue comme une sanction**.

La commission a adopté l'article ainsi modifié.

CHAPITRE IV
DISPOSITIONS DIVERSES D'APPLICATION

Article 38
Alléger le contrôle des biens de cryptologie

Cet article vise à alléger le contrôle des moyens et prestations de cryptologie, en particulier en passant d'un dispositif d'autorisation à un régime de déclaration préalable en matière d'exportation.

La commission a adopté cet article sans modification.

I. La situation actuelle – l'importation de bien de cryptologie est soumis à un dispositif d'information préalable et leur exportation à un dispositif de déclaration préalable auprès du Premier ministre

Le titre III de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (articles 29 à 46 de cette loi) est consacré à **la sécurité dans l'économie numérique** et le chapitre Ier de ce titre **aux moyens et prestations de cryptologie**.

1) Définition des moyens de cryptologie

Le premier article de ce chapitre Ier, l'article 29, précise qu'on entend par **moyen de cryptologie tout matériel** ou **logiciel** conçu ou modifié pour **transformer des données**, qu'il s'agisse **d'informations ou de signaux**, à **l'aide de conventions secrètes** ou pour **réaliser l'opération inverse avec ou sans convention secrète**.

Ces moyens de cryptologie ont principalement pour objet de **garantir la sécurité du stockage** ou **de la transmission de données**, en permettant **d'assurer leur confidentialité**, **leur authentification** ou **le contrôle de leur intégrité**.

On entend par **prestation de cryptologie** toute opération visant à **la mise en œuvre**, **pour le compte d'autrui**, **de moyens de cryptologie**.

2) Utilisation, fourniture, transfert, importation et exportation de moyens de cryptologie

L'article 30 la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est consacré à **l'utilisation**, à **la fourniture**, au **transfert**, à **l'importation** et à **l'exportation de moyens de cryptologie**.

Il prévoit que **l'utilisation des moyens de cryptologie est libre**, quelle que soit leur fonction.

La fourniture, **le transfert depuis ou vers un État membre de la Communauté européenne**, **l'importation** et **l'exportation** des moyens de

cryptologie **assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont également libres**.

Toutefois, **la fourniture**, **le transfert depuis un État membre de la Communauté européenne** ou **l'importation** d'un moyen de cryptologie **n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité** sont soumis à **une déclaration préalable** auprès du Premier ministre.

Le fournisseur ou la personne procédant au transfert ou à l'importation tiennent à la disposition du Premier ministre **une description des caractéristiques techniques de ce moyen de cryptologie**, ainsi que **le code source des logiciels utilisés**.

Un décret en Conseil d'État fixe :

- les conditions dans lesquelles sont souscrites **ces déclarations**, les conditions et les délais dans lesquels le Premier ministre peut demander **communication des caractéristiques du moyen**, ainsi que la nature de ces caractéristiques ;

- **les catégories de moyens** dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État, leur fourniture, leur transfert depuis un État membre de la Communauté européenne ou leur importation **peuvent être dispensés de toute formalité préalable**.

Le transfert vers un État membre de la Communauté européenne et **l'exportation d'un moyen de cryptologie** n'assurant **pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité** sont pour leur part soumis à **autorisation du Premier ministre**, et **non à simple déclaration préalable**.

Un décret en Conseil d'État fixe :

- Les conditions dans lesquelles sont souscrites **les demandes d'autorisation** ainsi que les délais dans lesquels le Premier ministre statue sur ces demandes ;

- **Les catégories de moyens** dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État, leur transfert vers un État membre de la Communauté européenne ou leur exportation peuvent être **soit soumis au régime déclaratif** et **aux obligations d'information** prévus ci-dessus, **soit dispensés de toute formalité préalable**.

Ce décret n° 2007-663 du 2 mai 2007 modifié, qui précise les modalités d'application de l'article 30, dispose notamment que **c'est à l'Agence nationale de sécurité des systèmes d'information (Anssi)** que **les déclarations et demandes d'autorisation d'exportation sont adressées**.

Il prévoit également que **les autorisations d'exportation** sont délivrées pour **une durée qui ne peut excéder cinq ans** et doivent être renouvelées passé ce délai.

Cette réglementation coexiste avec celle relative **aux biens à double usage (BDU)**, à savoir **les biens**, **produits** ou **technologies essentiellement civils**, sujets **au risque de détournement d'usage à des fins militaires prohibées** ou **de prolifération nucléaire**, **biologique** ou **chimique**, dont **l'exportation est contrôlée**. **Certains moyens de cryptologie sont également soumis à cette réglementation des BDU**.

Aussi, lorsqu'**un BDU intègre un dispositif de cryptologie**, il **faut une autorisation préalable d'exportation de bien de cryptologie** délivrée par l'Anssi, puis **une autorisation de licence d'exportation de BDU** relevant du régime général.

La réglementation européenne est notamment précisée par le décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert des biens et technologies à double usage (modifié pour tenir compte du règlement européen de 2009) et par l'arrêté du 13 décembre 2001 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les États membres de la Communauté européenne de biens et technologies à double usage.

Ce dernier texte précise que **l'autorisation d'exportation est un préalable à une demande de licence pour les moyens de cryptologie**. **Ce contrôle en deux étapes** ayant chacune **leurs délais propres** est donc perçu par les entreprises concernées comme **un double contrôle pénalisant pour l'export depuis la France**.

3) Responsabilité civile des prestataires de services de certification électronique pour les préjudices qu'ils causent

L'article 33 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique prévoit que sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, **les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés** dans chacun des cas suivants :

- **les informations** contenues dans le certificat, à la date de sa délivrance, étaient **inexactes** ;
- **les données** prescrites pour que le certificat puisse être regardé comme qualifié étaient **incomplètes** ;
- la délivrance du certificat **n'a pas donné lieu à la vérification** que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;

- les prestataires **n'ont pas**, le cas échéant, **fait procéder à l'enregistrement** de la révocation du certificat et tenu cette information à la disposition des tiers.

Les **prestataires ne sont pas responsables du préjudice causé** par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs.

Ils doivent justifier **d'une garantie financière suffisante**, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

4) Sanctions pénales en cas de non-respect des dispositions de l'article 30 relatives à l'utilisation, à la fourniture, au transfert, à l'importation et à l'exportation de moyens de cryptologie

L'article 34 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique prévoit **les sanctions administratives** associées **au non-respect de l'article 30** relatives à l'utilisation, à la fourniture, au transfert, à l'importation et à l'exportation de moyens de cryptologie.

Le I de l'article 35 prévoit **lui les sanctions pénales qui s'appliquent en cas de non-respect des dispositions de l'article 30**.

En premier lieu, **le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 30** en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au Premier ministre prévue par ce même article **est puni d'un an d'emprisonnement et de 15 000 euros d'amende**.

En second lieu, **le fait d'exporter un moyen de cryptologie** ou de **procéder à son transfert vers un État membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30** ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, **est puni de deux ans d'emprisonnement et de 30 000 euros d'amende**.

II. Le dispositif envisagé – le passage d'un régime d'autorisation à un simple régime de déclaration préalable pour l'exportation de moyens de cryptologie

L'article 38 du présent projet de loi procède à **une réécriture complète de l'article 30** de la loi n° 2004-575 du 21 juin 2004[1] consacré à l'utilisation, à

[1] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)*

la fourniture, au transfert, à l'importation et à l'exportation **de moyens de cryptologie**.

Il procède également à **une abrogation de l'article 33** et **modifie le I de l'article 35**.

L'objectif de ces évolutions législatives est **d'alléger la charge qui pèse sur les entreprises et l'administration en matière de contrôle des moyens de cryptologie**.

1) Évolution des dispositions relatives à l'utilisation, la fourniture, le transfert, l'importation et l'exportation de moyens de cryptologie

Le I de l'article 30 réécrit demeure inchangé et prévoit toujours que **l'utilisation des moyens de cryptologie est libre**.

Le II, qui prévoit que la fourniture, le transfert depuis ou vers un État membre de l'Union européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres, demeure lui aussi inchangé à l'exception de **l'actualisation consistant à remplacer les mots « *Communauté européenne* » par les mots « *Union européenne* »**.

Le III prévoit que **la fourniture**, **le transfert depuis ou vers un État membre de l'Union européenne**, **l'importation et l'exportation** d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à **une déclaration préalable** auprès du Premier ministre, **sans préjudice des exigences applicables aux biens à double usage intégrant un moyen de cryptologie**.

Un décret en Conseil d'État fixe :

- Les conditions dans lesquelles sont souscrites **ces déclarations**, les conditions et les délais dans lesquels le Premier ministre peut demander **communication des caractéristiques du moyen**, ainsi que **la nature de ces caractéristiques** ;
- Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, **au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État**, **leur fourniture**, **leur transfert** depuis ou vers un État membre de l'Union européenne ou **leur importation** ou **exportation** peuvent être **dispensés de toute formalité préalable**.

Ce nouveau III rassemble les dispositions relatives à **l'importation de moyens de cryptologie** de l'ancien III et celles relatives à **l'exportation de moyens de cryptologie** de l'ancien IV.

Trois évolutions notables méritent d'être notées.

La première, et de loin la plus importante, est **le passage d'un régime d'autorisation à un simple régime de déclaration préalable pour l'exportation de moyens de cryptologie**.

Il s'agit là d'une mesure de simplification car **le régime d'autorisation préalable à l'exportation de moyens de cryptologie** poursuit pour l'essentiel **le même objectif que le régime d'autorisation préalable à l'exportation des biens à double usages** prévu par le règlement 2021/821.

En outre, même si elle ne simplifie pas les démarches imposées pour l'importation et la fourniture en France de moyens de cryptologie, cette évolution permet néanmoins, grâce **au régime unique de déclaration applicable à toutes les opérations**, d'alléger la charge pour l'administration tout en maintenant **un dispositif de contrôle et de recueil d'informations techniques** sur **les moyens de cryptologie circulant en France**.

En deuxième lieu, l'obligation qui était faite au fournisseur ou à la personne procédant au transfert ou à l'importation de tenir à la disposition du Premier ministre **une description des caractéristiques techniques du moyen de cryptologie**, ainsi que **le code sources des logiciels utilisés**, **disparaît**.

En troisième lieu, il est précisé que les règles du nouveau III s'appliquent **sans préjudice des exigences applicables aux biens à double usage intégrant un moyen de cryptologie**, afin de prendre en compte **le régime d'autorisation préalable à l'exportation des biens à double usages (BDU)** prévu par le règlement 2021/821, pour lequel **un dispositif d'autorisation d'exportation sera bien maintenu**.

2) Responsabilité des prestataires de services de certification électronique pour les préjudices qu'ils causent

L'article 33 qui prévoyait que, sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, **les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes** qui se sont **fiées raisonnablement aux certificats présentés par eux** comme qualifiés est abrogé.

Comme rappelé *supra*, cet article 33 prévoyait **un régime de responsabilité civile des prestataires de services de certification électronique**.

Les principes énoncés dans cet article étaient devenus **obsolètes** et **en partie incohérents** avec les dispositions prévues à l'article 13 du règlement européen 910/2014 dit « eIDAS ».

En effet, l'article 33 de la loi n° 2004-575 prévoyait que « *Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence,* ***les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux*** *comme qualifiés* […] ».

Le règlement eIDAS, quant à lui, prévoit à son article 13 **un régime général de responsabilité du prestataire de service de confiance**, que **ce dernier soit qualifié ou non** : « *Sans préjudice du paragraphe 2, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou*

par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le [*règlement eIDAS*] ».

L'abrogation de l'article 33 constitue donc **une mesure de simplification et de clarification juridique**.

3) Sanctions pénales en cas de non-respect des dispositions de l'article 30 relatives à l'utilisation, à la fourniture, au transfert, à l'importation et à l'exportation de moyens de cryptologie

Le I de l'article 35 de la loi n°2004-575 est réécrit par le présent article 38 pour prévoir que sans préjudice de l'application du code des douanes, **le fait de ne pas satisfaire à l'obligation prévue à l'article 30 de la même loi** en cas de fourniture, de transfert depuis ou vers un État membre de l'Union européenne, d'importation ou d'exportation d'un moyen de cryptologie **est puni d'un an d'emprisonnement et de 15 000 euros d'amende**.

L'absence de respect de l'obligation de communication au Premier ministre prévue à l'article 30 **n'est donc plus sanctionnée**.

De même, **la sanction qui était prévue en cas d'exportation d'un moyen de cryptologie** ou son transfert vers un État membre de l'Union européenne **sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30** ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, **disparaît**. Cette sanction était **de deux ans d'emprisonnement et de 30 000 euros d'amende**.

III. La position de la commission – une mesure de simplification bienvenue pour éviter un dispositif de double autorisation à l'export inutile

Le régime d'autorisation préalable à l'exportation de moyens de cryptologie prévu par la loi n° 2004-575 pour la confiance dans l'économie numérique actuellement en vigueur poursuit **le même objectif que le régime d'autorisation préalable à l'exportation des biens à double usages (BDU)** prévu par le règlement 2021/821.

Il en résulte, pour **les entreprises qui exportent des biens à double usage (BDU) contenant des moyens de cryptologie**, **une double procédure d'autorisation** alors qu'il s'agit **d'une même opération d'exportation**.

Cette situation génère **beaucoup d'incompréhension de la part des entreprises concernées**, car elles sont **pénalisées** par **ce surcroît de formalités administratives** qui **rallonge les délais** en amont de la commercialisation de leur produits et **nuit à leur compétitivité vis-à-vis de leurs concurrents étrangers**.

En ce qui concerne l'Anssi, **le traitement des demandes d'autorisation d'exportation** prévues par la loi n° 2004-575 pour la confiance dans l'économie numérique, qui vient s'ajouter **aux demandes d'autorisation**

d'exportation de biens à double usage (BDU), constitue **une charge aussi chronophage que peu utile**.

De fait, ce sont aujourd'hui **trois équivalents temps plein (ETP) qui doivent traiter cinq cent demandes d'autorisation d'exportation de moyens de cryptographie par an**, les fonctions de cryptographie étant aujourd'hui présentes dans de nombreux produits.

Or, ainsi que cela a été précisé par l'Anssi à votre rapporteur, **au cours des cinq dernières années, aucun refus n'a été délivré en réponse à une demande d'autorisation d'exportation** déposée en application de la loi n° 2004-575 précitée, ce qui tend à montrer que, dans les faits, **ce dispositif n'a pas lieu d'être**.

La transformation de ce régime d'autorisation en régime déclaratif constitue donc **une mesure de simplification bienvenue**, à même de contribuer à **l'amélioration de la compétitivité des entreprises qui exportent des moyens de cryptographie ou des produits qui en contiennent**, grâce à **un allègement des procédures administratives** et à **un raccourcissement des délais**, et de **libérer l'Anssi de ce travail**, pour **redéployer ses ressources vers ses nombreuses autres missions**.

La suppression des sanctions prévues en cas de défaut d'obtention d'autorisation apparaît pleinement **cohérente** avec la suppression du régime d'autorisation lui-même.

La commission a adopté cet article sans modification.

Article 39

Abrogation de la transposition de la directive NIS 1 et simplification du cadre réglementaire

Cet article vise à abroger la transposition de la directive NIS 1 et à procéder à une simplification du cadre réglementaire, pour tenir compte de la transposition de la directive NIS 2 assurée par le présent projet de loi.

La commission a adopté cet article modifié par un amendement rédactionnel.

I. La situation actuelle – plusieurs textes portant sur la cybersécurité, et en particulier les dispositions législatives de transposition de la directive NIS 1, doivent être supprimés ou modifiés pour tenir compte de la transposition de la directive NIS 2

Dans le contexte de **la transposition de la directive NIS 2** assuré par le présent projet de loi, **de nombreuses dispositions législatives** deviennent **caduques** et doivent par conséquent **être abrogées**.

I) Le titre Ier de la loi n° 2018-133 du 26 février 2018 assure la transposition en droit français de la directive NIS 1

Le titre Ier, soit les articles 1 à 15, de la loi n° 2018-133 du 26 février 2018 **transpose en droit national** les dispositions de la directive n° 2016/1148 du 6 juillet 2016 dite **NIS 1**, dont l'objectif majeur était d'assurer **un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne**.

Prenant pour modèle **le volet cyber du dispositif national de sécurité des activités d'importance vitale (SAIV)** prévu par le code de la défense, cette loi prévoit **la désignation d'opérateurs de services essentiels (OSE)**.

Ces OSE sont désignés par le Premier ministre au regard de leurs activités, qui s'inscrivent **dans un secteur défini dans la transposition nationale** et reprenant au minimum **ceux listés dans la directive NIS 1**.

Ces OSE sont tenus de **déclarer à l'Agence nationale de sécurité des systèmes d'information (Anssi) leurs systèmes d'information essentiels (SIE)** répondant à des critères définis au niveau réglementaire et sur lesquels ces opérateurs doivent appliquer des mesures de sécurité.

Les mesures de sécurité définies dans le cadre de NIS 1 reprennent **celles définies dans le cadre du volet cyber du dispositif SAIV** et dont les exigences ont été **allégées** pour tenir compte **des enjeux visés par la directive** et **de la maturité des OSE**.

Cette loi vise également **les fournisseurs de services numériques** qui couvrent les services d'informatique en nuage (opérateurs de *cloud*), **les places de marché en ligne** et **les moteurs de recherche**.

II) L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

L'ordonnance n° 2005-1516 du 8 décembre 2005 introduit **le référentiel général de sécurité (RGS)** qui impose **aux autorités administratives** la mise en œuvre **de mesures de sécurité** visant à **limiter la fraude liée à l'usage des services numériques de ces administrations pour échanger avec leurs usagers** ou **d'autres administrations** (par exemple : l'identification électronique, la signature ou le cachet électronique, l'horodatage électronique)[1].

Trois types d'acteurs sont concernés par le RGS :

- **L'autorité administrative** qui se voit imposer **des obligations dans ces échanges par voie électronique** avec ses usagers ou d'autres autorités administratives ;
- **Les prestataires de services de confiance** ou **des fournisseurs** qui peuvent, sur la base du volontariat**, qualifier leurs produits de sécurité** ou **leurs services de confiance** en vue de les proposer aux autorités administratives pour faciliter leur mise en conformité aux obligations ;
- **Les organismes** délivrant **des décisions de qualification des prestataires de services de confiance**.

Le RGS s'applique **aux seuls systèmes d'information mis en œuvre par les autorités administratives** et qui **supportent des échanges par voie électronique entre ces autorités administratives et leurs usagers** ou **entre autorités administratives elles-mêmes** (par exemple : impots.gouv.fr ou le site internet d'une collectivité territoriale permettant à un administré de payer les frais de cantine).

Lorsqu'une autorité administrative recourt à **des produits de sécurité** ou à **des prestataires de services de confiance** ayant fait l'objet **d'une qualification**, cette administration peut **se prévaloir d'une présomption de conformité aux exigences du RGS**.

III) Les dispositions du code des postes et des communications électroniques portant sur les opérateurs de communication électronique et sur les offices d'enregistrement

Plusieurs dispositifs **du code des postes et des communications électroniques (CPCE)** sont directement concernés par les articles du titre II du présent projet de loi, raison pour laquelle l'article 39 leur apporte les modifications qui seront exposées *infra*.

---

[1] *L'ordonnance n° 2005-1516 du 8 décembre 2005 s'accompagne du décret 2010-112 du 2 février 2010 et de l'arrêté du 13 juin 2014 portant approbation de la dernière version RGS.*

En premier lieu, l'article L. 33-1 du code des postes et des communications électroniques prévoit que **l'établissement et l'exploitation des réseaux ouverts au public** et **la fourniture au public de services de communications électroniques** sont **libres** sous réserve **du respect de règles** portant notamment sur **les conditions de permanence**, **de qualité**, **de disponibilité**, **de sécurité** et **d'intégrité du réseau et du service** qui incluent **des obligations de notification** à l'autorité compétente **des incidents de sécurité** ayant eu **un impact significatif sur leur fonctionnement**.

En deuxième lieu, les articles L. 45 et suivants portent sur **l'attribution et la gestion des noms de domaine** et sur **les offices d'enregistrement**, sujets traités par les articles 18 à 22 du projet de loi.

II. Le dispositif envisagé – l'abrogation ou la modification de plusieurs textes portant sur la cybersécurité

1) Suppression des références à la loi n° 2018-133 transposant la directive NIS 1 dans le code de la défense

Le titre I^er^ de la loi n° 2018-133 transposant la directive NIS 1 étant abrogé par le III du présent article 39 du projet de loi, le I dudit article 39 **procède au remplacement de la référence** « loi n° 2028-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité » par **les mots « loi n°…. du …. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité »**.

Cette évolution est directement liée au fait que **les OIV et les OSE** mentionné aux L. 2321-2-1 et L. 2321-3 du code de la défense **sont remplacés par la notion d'entité « essentielle »** prévue par la transposition de la directive NIS 2.

2) La modification des dispositions du code des postes et des communications électroniques portant sur les opérateurs de communication électronique et sur les offices d'enregistrement

Le II de l'article 39 apporte des modifications à plusieurs articles du code des postes et des communications électroniques (CPCE) relatifs **aux modalités d'enregistrement des noms de domaine de premier niveau**.

Le 1° remplace la mention de la déclaration des incidents prévue à l'article L. 33-1 par un r) faisant référence au présent projet de loi. L'objectif est ainsi de **supprimer**, au sein du CPCE, **les dispositions spéciales concernant la cybersécurité en matière de communications électroniques** afin de les intégrer dans le droit général prévu par le présent projet de loi.

La modification de l'article L. 33-1 du CPCE rend ainsi **applicable**, en droit interne, **aux opérateurs de télécommunication**, **l'ensemble des**

dispositions prévues par le projet de loi. Il est précisé que ces dispositions sont applicables en Polynésie française, dans les îles Wallis et Futuna et en Nouvelle-Calédonie.

Le 2° du II de l'article 39 précise à l'article L. 45 du CPCE que **chaque office d'enregistrement** est **responsable du fonctionnement technique du domaine de premier niveau** qui lui est attribué, incluant notamment **l'exploitation** de ses serveurs de noms de domaine, **la maintenance** de ses bases de données d'enregistrement et **la distribution** des fichiers de zone du domaine de premier niveau sur les serveurs de noms de domaine, qu'il effectue ces opérations lui-même ou qu'elles soient sous traitées.

Le 3° apporte **une précision rédactionnelle** à l'article L.45-3 du CPCE.

Le 4° ajoute des références **aux agents agissant pour le compte des bureaux d'enregistrement** à l'article L. 45-4 du CPCE et prévoit qu'un décret en Conseil d'État **vient préciser les catégories auxquelles appartiennent lesdits agents**.

Le 5° modifie l'article L. 45-5 du CPCE pour prévoir que les offices d'enregistrement, par l'intermédiaire des bureaux d'enregistrement ainsi que des agents agissant pour le compte de ces derniers, **collectent les données nécessaires à l'enregistrement des noms de domaine**, notamment celles **relatives à l'identification des personnes physiques ou morales titulaires de ces noms de domaine** et des personnes chargées de leur gestion. Après leur enregistrement, et sans retard injustifié, **les offices et les bureaux d'enregistrement rendent publiques**, au moins quotidiennement, **ces données dès lors qu'elles n'ont pas de caractère personnel**. Ils tiennent **ces bases de données à jour**, en maintenant les données exactes et complètes, sans redondance de collecte, et sont responsables du traitement de ces données dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le 5° prévoit également que **les offices et les bureaux d'enregistrement** répondent aux demandes d'accès aux données d'enregistrement **dans un délai n'excédant pas soixante-douze heures après réception de la demande**. Il précise que la liste des données d'enregistrement devant être collectée est fixée par décret en Conseil d'État.

3) <u>L'abrogation du titre I^er^ de la loi n° 2018-133 transposant la directive NIS 1</u>

L'article 44 de la directive 2022/2555 dite NIS 2 vient **abroger les dispositions de la directive (UE) 2016/1148 dite NIS 1**.

En conséquence, le III de l'article 39 du projet de loi prévoit **l'abrogation du titre I^er^ de la loi n° 2018-133 transposant la directive NIS 1**.

L'abrogation de ce titre constitue donc **la traduction logique de la disparition de la directive qu'il avait transposé en droit français**.

4) Abrogation de plusieurs articles de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Le IV de l'article 39 procède à **l'abrogation de plusieurs articles** de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qui, comme rappelé *supra*, **avait introduit le référentiel général de sécurité (RGS)** qui impose aux autorités administratives la mise en œuvre **de mesures de sécurité visant à limiter la fraude liée à l'usage des services numériques de ces administrations pour échanger avec leurs usagers ou d'autres administrations**.

Dans un souci de simplification et d'harmonisation des exigences applicables, **seules les administrations qui seront assujetties à la transposition nationale de la directive NIS 2 seront par ailleurs assujetties au RGS**.

Le RGS conservera son périmètre technique actuel, à savoir les systèmes d'information que les administrations mettent en œuvre et qui supportent des échanges par voie électronique entre ces administrations et leurs usagers ou entre administrations elles-mêmes.

Les dispositions de l'article 9 de l'ordonnance n° 2005-1516 définissant **les obligations pour les autorités administratives sont abrogées** car désormais portées par les dispositions de l'article 14 du projet de loi.

En supprimant le raccrochement du RGS à l'article 9 de l'ordonnance n° 2005-1516 et **en le couvrant via les dispositions du troisième alinéa de l'article 16** du projet de loi, les dispositions du IV de l'article 39 du projet de loi permettent de :

- **Modifier le champ d'application du RGS** pour ne couvrir que les administrations visées par la transposition de la directive NIS 2.
- **Définir des mesures de sécurité spécifiques**, pour les systèmes d'information supportant des échanges par voie électronique entre l'administration mettant en œuvre un tel système et les usagers de ce système d'information ou d'autres administrations, visant à **limiter la fraude liée à l'usage de ces systèmes d'information**.

Les dispositions de l'article 12 de l'ordonnance n° 2005-1516 relatives **au référencement des produits de sécurité** et **prestataires de services de confiance qualifiés** sont **abrogées car abandonnées**.

Un impact économique positif bénéficiera aux prestataires de services de confiance dont **la qualification au titre du règlement eIDAS** leur permettra **d'être conforme aux exigences du RGS**, **les dispensant** ainsi de

s'engager dans un second processus de qualification au titre du RGS long et onéreux.

Les dispositions du I de l'article 14 de l'ordonnance n° 2005-1516 relatives au délai de mise en conformité au RGS **sont abrogées**.

Les définitions des notions utilisées dans les articles abrogés mentionnés précédemment, à savoir celles au 2° et 3° du II de l'article 1er de l'ordonnance n° 2005-1516 **sont également abrogées**.

III. La position de la commission – des abrogations et de modifications de textes qui permettent de simplifier le droit et de prendre en compte les modifications apportées par le titre II du présent projet de loi

Le présent article 39 porte des mesures destinées à **adapter plusieurs textes** pour tenir compte **des dispositions adoptées au titre II du projet de loi pour transposer la directive NIS 2**.

C'est bien sûr le cas de **l'abrogation du titre Ier de la loi n° 2018-133 transposant la directive NIS 1** qui n'avait plus lieu d'être une fois la directive NIS 2 transposée.

Mais c'est également le cas des articles L. 45 et suivants du code des postes et des communications électroniques (CPCE) qui devaient être **modifiés pour tenir compte des dispositions des articles 18 à 22 du projet de loi sur les offices et bureaux d'enregistrement** ou de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qu'il fallait revoir en particulier pour **concilier le champ d'application du Règlement général de sécurité (RGS) et celui de NIS 2**, de sorte que **les administrations ne soient pas visées par un double dispositif d'obligations**.

Au total, **cet article technique** n'a donc **pas appelé de modifications** de fond de la part de la commission spéciale, à l'exception d'un amendement rédactionnel COM 122 du rapporteur Patrick Chaize.

La commission a adopté cet article ainsi modifié.

Article 40
Mesures applicables à l'outre-mer pour les territoires sous spécialité législative

Cet article vise à étendre l'application du titre II du présent projet de loi aux collectivités d'outre-mer régies par le régime de spécialité législative

La commission a adopté un amendement relatif à l'application d'une partie de ses dispositions en Nouvelle-Calédonie et en Polynésie française.

La commission a adopté cet article ainsi modifié.

I. La situation actuelle – la loi de transposition de la directive NIS 1 était directement applicable dans les collectivités d'outre-mer régies par le régime de l'identité législative et prévoyait des mesures spécifiques pour les collectivités régies par le régime de spécialité législative

Comme indiqué précédemment, **la directive européenne NIS 1** avait été transposée en droit français au moyen de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

Les mesures prévues par cette loi étaient **directement applicables aux collectivités régies par le régime de l'identité législative**, c'est-à-dire le département de Guadeloupe, le département de La Réunion, les régions de la Guadeloupe et de La Réunion, les collectivités de la Guyane, de la Martinique et de Mayotte, mais également Saint-Barthélemy, Saint-Pierre-et-Miquelon et Saint-Martin.

Il avait fallu en revanche **adopter des mesures spécifiques pour les collectivités régies par le régime de spécialité législative**, pour lesquelles seules les dispositions législatives qui comportent une mention expresse à cette fin sont applicables dans ces territoires, à savoir les îles Wallis-et-Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises.

II. Le dispositif envisagé – des dispositions destinées à prévoir l'application du titre II du présent projet de loi aux collectivités d'outre-mer régies par le régime de spécialité législative

Alors que les territoires d'outre-mer sont de plus en plus connectés et confrontés à des cyber menaces, les articles du titre II du présent projet de loi assurant la transposition de la directive NIS 2 **sont applicables de plein droit**, **sans aucune adaptation**, **aux collectivités régies par le régime de l'identité législative**, c'est-à-dire le département de Guadeloupe, le département de La Réunion, les régions de la Guadeloupe et de La Réunion, les collectivités de la

Guyane, de la Martinique et de Mayotte, mais également Saint-Martin **car ces collectivités font toutes parties du territoire de l'Union européenne**.

En vertu **du régime de spécialité législative**, le I du présent article 40 dispose expressément que le titre II du présent projet de loi, à l'exception de son article 13, est **applicable dans les îles Wallis-et-Futuna**, **en Polynésie française**, **en Nouvelle-Calédonie** et dans **les Terres australes et antarctiques françaises**, sous réserve des adaptations suivantes :

- en l'absence d'adaptation, les références faites, par des dispositions du titre II applicables en Polynésie française et en Nouvelle-Calédonie, à des dispositions qui n'y sont pas applicables sont remplacées par **les références aux dispositions ayant le même objet applicable localement** ;
- dans les îles Wallis-et-Futuna, en Polynésie française et en Nouvelle-Calédonie, **les sanctions pécuniaires** encourues en vertu du titre II du présent projet de loi sont **prononcées en monnaie locale**, compte tenu de la contre-valeur de l'euro dans cette monnaie.

Le II de l'article 40 prévoit également que l'article 13 du présent projet de loi **n'est pas applicable à Saint-Barthélemy et à Saint-Pierre-et-Miquelon**. De fait, l'article 13 du projet de loi, en ce **qu'il renvoie à des textes sectoriels non visés explicitement** (existants ou à venir) **ne peut être applicable aux pays et territoires d'outre-mer (PTOM)** conformément aux principes d'identité et spécialité législative selon les collectivités et territoires.

C'est également **afin de respecter l'inapplicabilité du droit de l'UE dans ces territoires** qu'il a été fait le choix de rendre applicables dans ces territoires les dispositions du titre II du projet de loi « *en tant que droit national faisant référence au droit dérivé* ». Le III de l'article 40 prévoit ainsi que pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis-et-Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, **les références à la directive NIS 2 et à d'autres textes européens** sont remplacées par **la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements**.

Au total, en matière de périmètre d'application, l'article 40 du projet de loi prévoit donc **une application sans restriction des éléments prescriptifs de la directive NIS 2** relatifs à **la définition des entités concernées**, **aux critères et seuils**, **aux secteurs**, **sous-secteurs et types d'entité dans toutes les collectivités d'outre-mer**.

Les dispositions des paragraphes IV à VI visent à **coordonner les textes** et à **assurer la cohérence outre-mer pour les textes respectifs suivants** :

- la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

- l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

III. La position de la commission – les entités des territoires ultra-marins doivent se voir appliquées les mêmes obligations en matière de cybersécurité que celles de l'hexagone, eu égard au niveau de menace cyber qui pèse également sur elles

Les territoires d'outre-mer disposent **d'un tissu économique** et **de collectivités territoriales de plus en plus numérisés et connectés**.

L'isolement de ces territoires, pour la plupart **insulaires**, et **l'éloignement de l'hexagone** se traduisent par **l'existence d'entités « essentielles »** et **« importantes »** dans **tous les secteurs « hautement critiques »** et **« critiques »** listés aux annexes I et II de la directive NIS 2 (énergie, transports, etc.).

Ces entités sont en moyenne **de taille plus réduite** que dans l'hexagone et sont **souvent en situation de monopole**, ce qui est **source de vulnérabilité** pour **l'économie** et **les sociétés des territoires ultra-marins**.

Il est donc essentiel que **les dispositions législatives transposant NIS 2** leur soient pleinement appliqués afin **d'élever leur niveau de cybersécurité au même niveau que celui applicable aux entités hexagonales**.

La commission spéciale a toutefois adopté un amendement COM 123 du rapporteur Patrick Chaize visant à **clarifier l'applicabilité en Nouvelle-Calédonie et en Polynésie française** des modifications du code des postes et des communications électroniques (CPCE) **en matière de noms de domaine** prévues au présent article 39.

La rédaction initialement proposée rend de fait applicable l'ensemble du titre II à la Nouvelle-Calédonie et à la Polynésie française ce qui inclue les modifications du CPCE prévues à l'article 39. Or **la gestion des noms de domaine locaux** (.pf, .nc) **relève des compétences propres de ces deux collectivités** et les articles modifiés du CPCE ne trouvent pas à s'y appliquer.

L'amendement adopté par la commission spéciale précise donc que le titre II s'applique en Nouvelle Calédonie et en Polynésie française **à l'exception des modifications des articles L45 et suivants du CPCE prévues par l'article 39 du projet de loi**.

De cette écriture résulte donc l'applicabilité suivante :

- le présent projet de loi, et notamment la section III du chapitre II relative aux noms de domaine, **s'applique dans l'ensemble des collectivités d'outre-mer** ;

- les mesures de coordination avec le CPCE prévues à l'article 39 s'appliquent pour les îles Wallis et Futuna ainsi que pour les Terres australes et antarctiques françaises **mais ne s'appliquent pas en Nouvelle-Calédonie et en Polynésie française**.

Ces dernières ne sont donc soumises **qu'aux obligations du présent projet de loi et de leurs codes respectifs pour ce qui concerne la gestion de noms de domaine locaux**.

La commission a adopté cet article ainsi modifié.

CHAPITRE V
« Dispositions relatives aux communications électroniques »

CHAPITRE V
DISPOSITIONS RELATIVES AUX COMMUNICATIONS ÉLECTRONIQUES

Article 41
Renforcement des sanctions pénales pour améliorer la lutte contre les brouillages

Cet article renforce les sanctions pénales pour améliorer la lutte contre les brouillages et les leurrages, insuffisamment sanctionnés aujourd'hui alors même que leurs conséquences sur la vie économique et sociale peuvent s'avérer très graves.

La commission a adopté cet article modifié par un amendement rédactionnel.

I. La situation actuelle – un niveau de sanction faible pour les activités prohibées susceptibles de brouiller les émissions hertziennes

1) Les principales activités susceptibles de brouiller les émissions hertziennes sont aujourd'hui punies de six mois d'emprisonnement et de 30 000 euros d'amende

La transmission hertzienne, c'est-à-dire **sur des liaisons sans fil** (réseaux de téléphonie mobile, réseaux professionnels privés, WIFI, etc.) **de données** ou **de la voix** joue aujourd'hui **un rôle essentiel** dans **la vie institutionnelle**, **économique et sociale** de notre pays, et **des secteurs majeurs d'activité** en sont dépendants **pour assurer leur bon fonctionnement**.

L'étude d'impact du projet de loi cite à titre d'exemples particulièrement éclairants **la couverture mobile des territoires**, **la connectivité des zones reculées**, **les services de surveillance à domicile de personnes âgées**, **les terminaux de paiement par carte**, **les appels d'urgence sur téléphone mobile** ou bien encore le fonctionnement **des radars de prévisions météorologiques**.

En raison de **l'importance cruciale de ces transmissions hertzienne**, **l'utilisation dans des conditions non conforme d'un appareil électrique**, **radioélectrique** ou **électronique** ou **d'une fréquence radioélectrique** ou l'utilisation délibérée **d'un brouilleur d'ondes** peut, **en perturbant des émissions hertziennes**, **compromettre le fonctionnement** de tous les services **utilisant les bandes de fréquences concernées** pour la transmission et la réception d'informations ou la communication vocale.

La lutte contre ces perturbations ou brouillages constitue dès lors un impératif pour **assurer le bon fonctionnement des services de**

communication par radiofréquences, tels que **la téléphonie** et **l'Internet mobiles**, **les services de communication utilisés par les services de défense nationale** et **les forces de sécurité et de secours**, **les communications des pilotes d'avion**, **les alertes de détresse pour l'aviation et le transport maritime**, **la réception de données de synchronisation et de temps via le GPS ou Galileo**[1], ainsi que des activités recourant à des communications ou à des échanges de données par voie hertzienne, tels que **les services de transport**, **la météorologie**, **les objets connectés**, **l'industrie 4.0**, **les infrastructures connectées** et **les territoires intelligents**.

Afin de **dissuader les auteurs de brouillage**, intentionnels ou non intentionnels, l'article L. 39-1 du code des postes et des communications électroniques dispose que sont **punis de six mois d'emprisonnement et de 30 000 euros d'amende** les faits ci-dessous.

En premier lieu, le fait de **maintenir un réseau indépendant en violation d'une décision de suspension** ou **de retrait du droit d'établir un tel réseau**.

En deuxième lieu, **le fait de perturber**, en utilisant une fréquence, un équipement ou une installation radioélectrique **les émissions hertziennes d'un service autorisé**.

Ce type de perturbation est illégale lorsque l'utilisation d'une fréquence, d'un équipement ou d'une installation radioélectrique se fait :

- dans des conditions non conformes aux dispositions de l'article L. 34-9 du même code des postes et des communications électroniques, lequel prévoit que **les équipement radioélectriques**, y compris ceux destinés à être connectés à un réseau ouvert au public, **doivent faire l'objet d'une évaluation de conformité** aux exigences essentielles qui leur sont applicables et doivent être à tout moment conformes à celles-ci. C'est l'Agence nationale des fréquences (ANFR) qui constitue **l'autorité de contrôle pour la surveillance du marché des équipements radioélectriques** ;
- ou **sans posséder l'autorisation** (ou en dehors des conditions de ladite autorisation lorsque celle-ci est requise) prévue à l'article L. 41-1 du même code délivrée par l'ANFR, lequel prévoit que l'utilisation de fréquences radioélectriques en vue d'assurer soit l'émission, soit à la fois l'émission et la réception de signaux, peut être **soumise à autorisation administrative de l'ANFR** lorsque cela est nécessaire pour **éviter les brouillages préjudiciables**, assurer la qualité technique du service, préserver l'efficacité de l'utilisation des fréquences radioélectriques ou pour réaliser un

[1] *Galileo est le GPS européen.*

objectif d'intérêt général. L'ANFR est en charge du contrôle de cette disposition ;

- ou **en dehors des conditions réglementaires générales** prévues à l'article L. 33-3 du même code, lequel prévoit que sous réserve de leur conformité aux dispositions du code des postes et des communications électroniques, les installations radioélectriques n'utilisant pas des fréquences spécifiquement assignées à leur utilisateur sont établies librement, donc ne nécessitent pas d'autorisation individuelle. Là encore, c'est l'ANFR qui assure le contrôle de cette disposition.
- ou **sans posséder le certificat d'opérateur** prévu à l'article L. 42-4 du même code, lequel dispose que le ministre chargé des communications électroniques détermine par arrêté les catégories d'installations radioélectriques d'émission pour la manœuvre desquelles **la possession d'un certificat d'opérateur est obligatoire** et les conditions d'obtention de ce certificat.

Ces dispositions sont sans préjudice de l'application de l'article 78 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, qui prévoit **des amendes de 75 000 euros** pour **le dirigeant de droit ou de fait d'un service de communication audiovisuelle ayant émis ou fait émettre sans disposer des autorisations requises**.

En troisième lieu, l'article L. 39-1 du code des postes et des communications électroniques dispose que **sont punis de six mois d'emprisonnement et de 30 000 euros d'amende le fait de perturber**, en utilisant un appareil, un équipement ou une installation, dans des conditions non conformes aux dispositions applicables en matière de compatibilité électromagnétique des équipements électriques et électroniques fixées dans le code de la consommation, **les émissions hertziennes d'un service autorisé**.

Là encore, ces dispositions sont sans préjudice de l'application de l'article 78 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, qui prévoit **des amendes de 75 000 euros** pour **le dirigeant de droit ou de fait d'un service de communication audiovisuelle ayant émis ou fait émettre sans disposer des autorisations requises**.

En quatrième lieu, l'article L. 39-1 du code des postes et des communications électroniques dispose que sont **punis de six mois d'emprisonnement et de 30 000 euros d'amende** le fait d'utiliser une fréquence, un équipement ou une installation radioélectrique **dans des conditions non conformes** aux dispositions de l'article L. 34-9 **ou sans posséder l'autorisation** prévue à l'article L. 41-1 **ou en dehors des conditions de ladite autorisation** lorsque celle-ci est requise **ou sans posséder le certificat d'opérateur** prévu à l'article L. 42-4 **ou en dehors des conditions réglementaires générales** prévues à l'article L. 33-3 **ou sans l'accord** mentionné au I de l'article L. 43, c'est-à-dire **l'accord que peut donner**

l'Agence nationale des fréquences (ANFR) pour l'exploitation d'une station radioélectrique.

Enfin, l'article L. 39-1 du code des postes et des communications électroniques dispose que sont **punis de six mois d'emprisonnement et de 30 000 euros d'amende** le fait d'avoir pratiqué l'une des activités prohibées par le I de l'article L. 33-3-1, à savoir **l'importation**, **la publicité**, **la cession à titre gratuit ou onéreux**, **la mise en circulation**, **l'installation**, **la détention** et **l'utilisation de tout dispositif destiné à rendre inopérants des appareils de communications électroniques de tous types**, tant pour l'émission que pour la réception, en dehors des cas et conditions prévus au II de cet article, c'est-à-dire **pour les besoins de l'ordre public**, **de la défense et de la sécurité nationale**, ou **du service public de la justice**.

2) Un nombre de cas de brouillages et une gravité en augmentation

Ces dernières années, **le nombre de cas de brouillage** (perturbations d'un service autorisé) **sont en augmentation**, puisqu'**entre 1 400 et 1 800 cas par an** sont signalés à l'ANFR.

En outre, l'ANFR signale que c**es brouillages peuvent avoir des conséquences de plus en plus graves** en raison de **l'évolution des technologies hertziennes** (introduction de la 5G en matière de téléphonie et d'internet), **de la densification des usages dans des bandes de fréquences en partage avec d'autres services** (WIFI 6), **d'une dépendance croissante à la bonne réception du GPS**, **du développement des objets et capteurs connectés** et **de l'industrie 4.0** et **de l'intensité de la présence d'équipements radioélectriques, électriques et électroniques**.

Les brouillages accidentels sont ceux causés par la victime elle-même, du fait d'un défaut d'ingénierie de l'installation perturbée (30 à 40 cas par an). On peut aussi considérer comme accidentelles **des saturations de bandes libres comme le WiFi**, lorsque trop d'utilisateurs sont actifs en même temps. Ces brouillages fréquents sont rarement déclarés à l'ANFR (moins de 5 cas par an) car ce phénomène est la contrepartie de l'accès libre à ces bandes.

Tous les autres brouillages traités par l'ANFR correspondent aux cas énumérés dans l'article L. 39-1 du code des postes et des communications électroniques (CPCE). **Ils sont considérés comme intentionnels et réprimés comme tels**, car ils découlent soit de l'utilisation d'une fréquence, d'un équipement ou d'une installation radioélectrique **en dehors des conditions légales ou réglementaires**, soit de **la mise en œuvre d'un appareil non conforme**.

3) L'utilisation croissante de brouilleurs et de systèmes de leurrage

Toutefois, le sujet le plus préoccupant est bien sûr **l'utilisation délibérée de brouilleurs** alors que la loi française prévoit **leur interdiction générale** : leur importation, la publicité en leur faveur, leur cession à titre

gratuit ou onéreux, leur mise en circulation, leur installation, leur détention et leur utilisation **est explicitement prohibée**.

Malgré cette interdiction, **de plus en plus de brouilleurs sont en circulation sur le territoire national**.

Ces outils sont **particulièrement dangereux** car leurs effets sont souvent **beaucoup plus puissants que ne l'imaginent leurs utilisateurs**. Ainsi, par exemple, un brouilleur de GPS utilisé par un employé qui veut empêcher la géolocalisation de son véhicule par son employeur **peut perturber des avions volant à 2 000 mètres d'altitude**.

Or, dans le domaine de l'aviation, le brouillage du GPS ou de Galileo peut **générer des situations à risques lors des phases d'approches à proximité des pistes d'un aéroport**, qui nécessitent **une grande précision de géolocalisation**, surtout en cas de mauvaises conditions météorologiques ou de relief accidenté. Il s'agit là **d'un risque majeur pour la sécurité de l'aviation civile ou militaire**.

Mais les brouilleurs sont également **de plus en plus utilisés par des délinquants** pour commettre **des infractions** et pourraient, utilisés par des terroristes, **constituer des outils de guerre électronique**.

Outre le brouillage, **les outils de leurrage des systèmes de navigation par satellites (GNSS)** du GPS ou de Galileo constituent **un autre sujet de préoccupation majeur et croissant**.

Le leurrage consiste à **envoyer de faux signaux sur les bandes GNSS pour tromper les récepteurs GNSS** que ce soit en matière d'information de géolocalisation ou d'horaire. Plus insidieux qu'un brouillage, un leurrage est lui aussi susceptible d'avoir **des conséquences très dommageables** dans **les domaines des transports et des réseaux de communication**.

3) Un système de sanctions aujourd'hui inefficace

La sanction maximale prévue au L 39-1 actuel du CPCE est **de 6 mois d'emprisonnement et 30 000 euros d'amende**. Ce quantum est considéré comme **faible dans l'échelle des sanctions pénales**. De ce fait, **les infractions constatées au titre de cet article donnent rarement lieu à des poursuites**. **80 % des procès-verbaux d'infraction transmis aux parquets sont classés sans suite. Un sentiment d'impunité en découle** et **nuit tant à la prévention qu'à la prise de conscience par les auteurs de la nature délictuelle de leurs actes**.

En outre, lorsque le tribunal judiciaire est saisi, **les peines sont minimes**. Par exemple, l'auteur d'un brouillage près de l'aéroport de Nantes qui avait en 2017 **perturbé plusieurs avions** n'a été condamné à l'issue de son procès **qu'à une amende de 1 500 euros**.

II. Le dispositif envisagé – un net durcissement du quantum des peines pour les différentes actions entraînant un brouillage des émissions hertziennes, et en particulier pour l'utilisation de brouilleurs ou le recours au leurrage

L'article 42 du présent projet de loi propose **une nouvelle rédaction de l'article L. 39-1 du code des postes et des communications électroniques (CPCE)**.

Il **conserve le libellé des infractions pénales** telles qu'elles étaient mentionnées dans la version actuelle de l'article L. 39-1 du CPCE mais prévoit **un durcissement des sanctions pénales associées à certaines infractions**.

1) Une sanction inchangée pour la simple utilisation d'une fréquence, d'un équipement ou d'une installation radioélectrique dans des conditions non conforme

En premier lieu, le I du nouvel article L. 39-1 du code des postes et des communications électroniques (CPCE) prévoit que **sera puni de six mois d'emprisonnement et de 30 000 euros d'amende** le fait de **maintenir un réseau indépendant en violation d'une décision de suspension** ou **de retrait du droit d'établir un tel réseau** ou bien le fait **d'utiliser une fréquence**, **un équipement** ou **une installation radioélectrique** :

- **dans des conditions non conformes** aux dispositions de l'article L. 34-9 du même CPCE ;

- **ou sans posséder l'autorisation** (ou en dehors des conditions de ladite autorisation lorsque celle-ci est requise) prévue à l'article L. 41-1 du même code ;

- **ou en dehors des conditions réglementaires générales** prévues à l'article L. 33-3 du même code ;

- **ou sans posséder le certificat d'opérateur** prévu à l'article L. 42-4 du même code.

Reste donc soumise à six mois d'emprisonnement et à 30 000 euros d'amende la simple utilisation d'une fréquence, d'un équipement ou d'une installation radioélectrique **dans des conditions non conforme**, même si cette utilisation **n'a pas engendré de perturbation des émissions hertziennes d'un service autorisé**.

Une nouvelle infraction est également créée, elle aussi **punie de six mois d'emprisonnement et de 30 000 euros d'amende** lorsqu'une station radioélectrique **ne respecte pas les caractéristiques déclarées lors de la demande d'accord ou d'avis**, prévue au I de l'article L. 43 du CPCE, préalable à son implantation.

2) Une sanction durcie en cas de perturbation des émissions hertziennes d'un service autorisé

Le II de la nouvelle rédaction de l'article L. 39-1 prévoit qu'est puni de **trois ans d'emprisonnement et de 75 000 euros d'amende** le fait de **perturber les émissions hertziennes d'un service autorisé** en utilisant **une fréquence**, **un équipement** ou **une installation radioélectrique** :

- **dans des conditions non conformes** aux dispositions de l'article L. 34-9 du même CPCE ;

- **ou sans posséder l'autorisation** (ou en dehors des conditions de ladite autorisation lorsque celle-ci est requise) prévue à l'article L. 41-1 du même code ;

- **ou en dehors des conditions réglementaires générales** prévues à l'article L. 33-3 du même code ;

- **ou sans posséder le certificat d'opérateur** prévu à l'article L. 42-4 du même code.

Ces sanctions plus élevées ciblent les cas où **une personne à perturbé les émissions hertziennes d'un service autorisé** en utilisant **une fréquence**, **un équipement** ou **une installation radioélectrique** dans **des conditions non conformes** ou **sans avoir les autorisations ou certificats requis**.

À la différence de la simple utilisation sanctionnée de **six mois d'emprisonnement et de 30 000 euros d'amende**, il faut donc **qu'une perturbation ait été engendrée** par ladite utilisation pour que la sanction puisse **s'élever à trois ans d'emprisonnement et 75 000 euros d'amende**.

Cette sanction pourra notamment être envisagée pour **des usages créant des risques pour la vie humaine**.

En outre, le fait que cette sanction atteigne trois ans d'emprisonnement permettra à l'ANFR de **solliciter le soutien d'un officier de police judiciaire (OPJ) pour certaines atteintes graves au fonctionnement des fréquences**.

En effet, en vertu de l'article 76 du code de procédure pénale, **un OPJ ne peut procéder à une perquisition dans le cadre d'une enquête préliminaire**, hors flagrance, **que si la sanction atteint au moins trois ans d'emprisonnement**.

3) Une sanction nettement plus sévère pour les cas les plus graves

Le III de la nouvelle rédaction de l'article L. 39-1 prévoit qu'est puni **de cinq ans d'emprisonnement et de 150 000 euros d'amende** le fait d'avoir pratiqué **l'une des activités prohibées** suivantes : **l'importation**, **la publicité**, **la cession à titre gratuit ou onéreux**, **la mise en circulation**, **l'installation**, **la détention** et **l'utilisation de tout dispositif** destiné à **rendre inopérants des appareils de communications électroniques de tous types**, tant pour **l'émission** que pour **la réception**, c'est-à-dire **des « brouilleurs »**.

Ce quantum maximal permettra donc de **sanctionner beaucoup plus sévèrement** qu'auparavant **les cas de brouillage volontaires voire offensifs**, mais également **toutes les actions susceptibles d'y contribuer en amont**, et notamment toutes celles permettant **de se procurer des brouilleurs**.

Est également visé par la même sanction de **cinq ans d'emprisonnement et de 150 000 euros d'amende** le fait d'utiliser, sans l'autorisation prévue au premier alinéa de l'article L. 41-1 attribuée par l'ANFR, **des fréquences attribuées par le Premier ministre** pour les besoins **de la défense nationale et de la sécurité publique** ou **d'utiliser une installation radioélectrique**, en vue **d'assurer la réception de signaux transmis sur ces mêmes fréquences**, sans l'autorisation administrative prévue au deuxième alinéa de l'article L. 41-1 et également attribuée par l'ANFR.

III. La position de la commission – un durcissement du quantum de peine qui était indispensable, en particulier pour lutter contre l'utilisation des brouilleurs et des outils de leurrage

La commission spéciale a **accueilli très favorablement** les dispositions du présent article 41 visant à **durcir fortement le quantum des peines** pour **réprimer plus sévèrement la perturbation des émissions hertziennes**.

De fait, celles-ci sont aujourd'hui **essentielles dans de multiples dimensions de la vie économique et sociale** et **leur perturbation** peut avoir **des conséquences très graves**, et notamment **mettre des vies en danger**.

Le cas de l'aviation civile, qui peut voir **les informations que reçoivent les pilotes altérées**, remettant ainsi en cause **la sécurité des vols**, est à cet égard particulièrement emblématique du type **de risques sévères que ces perturbations peuvent engendrées**.

Si le maintien des sanctions actuelles pour l'utilisation non conforme d'une fréquence ou d'un matériel dès lors **qu'aucune perturbation n'a été constatée est acceptable**, il était indispensable de **punir plus sévèrement** les cas où **une perturbation des émissions hertziennes d'un service autorisé a été constatée**.

Il était surtout **inacceptable que l'utilisation délibérée de brouilleurs** ou **d'outils de leurrage**, et toutes les actions permettant de se procurer **ces outils prohibés**, soit **aussi peu sanctionnée** alors même qu'ils sont **dangereux pour la sécurité des personnes et des biens** et doivent être **réservés aux forces armées** ou **aux forces de sécurité intérieure**.

La commission spéciale a donc **approuvé dans réserve la nécessaire mise au jour de ce quantum de peines**, adoptant uniquement un amendement rédactionnel COM 124 du rapporteur Patrick Chaize.

La commission a adopté l'article sans modification.

Article 42

Renforcement des conditions d'accès à une assignation de fréquences déposée par la France auprès de l'Union internationale des télécommunications

Cet article vise à renforcer les conditions d'accès à une assignation de fréquences déposée par la France auprès de l'Union internationale des télécommunications (UIT).

La commission a adopté l'article 42 avec un amendement de précision rédactionnelle.

I. La situation actuelle – les entreprises font appel à l'ANFR pour obtenir une autorisation d'assignation de fréquence relative à un système satellitaire

Pour **transmettre des données** (imagerie, télécommunication, etc.) et pouvoir être contrôlés à distance, **les systèmes satellitaires orbitaux**[1] **communiquent avec des équipements placés sur Terre** grâce à **l'émission et à la réception d'ondes radioélectriques** qui utilisent **des bandes de fréquences spécifiques à chaque satellite**.

Les positions orbitales des satellites ainsi que **les fréquences associées** (ensemble dénommé « *filing* ») permettant de **communiquer entre les satellites géostationnaires et non géostationnaires** et **les stations terriennes** constituent **une ressource rare**[2].

Afin **d'en garantir la disponibilité** et **éviter ainsi les risques de brouillage entre satellites**, **l'Union Internationale des Télécommunications (UIT)**, agence de l'ONU spécialisées dans les technologies de l'information et de la communication met en œuvre **un processus** - préalable à tout lancement de satellites - **de déclaration des fréquences associées**.

Le règlement des radiocommunications (RR), révisé par les États membres à chaque Conférence mondiale des radiocommunications, **décrit précisément les procédures**, y compris la coordination entre États membres, visant à **assurer la disponibilité des fréquences** et **l'absence de brouillage**.

En pratique, il revient aux États de **déposer auprès de l'Union Internationale des Télécommunications (UIT) une demande d'enregistrement** portant à la fois sur **une ou plusieurs bandes de fréquences** et sur **une position orbitale donnée**.

En cas de problématique de coexistence, **l'utilisateur de la demande d'enregistrement la plus ancienne est prioritaire** vis-à-vis des autres

[1] *Ensemble de satellites artificiels mis en orbite dans l'espace extra-atmosphérique.*

[2] *On estime généralement entre quatre et six le nombre maximal de constellations de grande ampleur, soit comptant plusieurs milliers de satellites, qui pourraient in fine cohabiter en orbite.*

utilisateurs, ces derniers devant adapter leurs émissions radioélectriques pour ne pas perturber l'activité du premier

L'article L. 43 du code des postes et des communications électroniques (CPCE) prévoit que **l'Agence nationale des fréquences (ANFR) prépare la position française** et **coordonne l'action de la représentation française dans les négociations internationales dans le domaine des fréquences radioélectriques**.

À ce titre, elle est en charge **de déposer**, **au nom de la France**, **des demandes d'enregistrement auprès de l'UIT**.

1) Les règles relatives à une demande d'autorisation d'assignation de fréquence relative à un système satellitaire

L'article L. 97-2 du code des postes et des communications électroniques (CPCE) prévoit que **toute demande d'assignation de fréquence** relative **à un système satellitaire** est adressée à **l'Agence nationale des fréquences (ANFR)**.

Sauf si l'assignation demandée n'est pas conforme au tableau national de répartition des bandes de fréquences (TNRBF) ou aux stipulations des instruments de l'Union internationale des télécommunications (UIT), **l'ANFR déclare**, **au nom de la France**, **l'assignation de fréquence correspondante à l'UIT** et engage **la procédure d'enregistrement** prévue par **le règlement des radiocommunications (RR)**, en en informant l'opérateur.

Lors de son audition par votre rapporteur, l'ANFR lui a expliqué **qu'un opérateur peut s'adresser à tout État membre de l'UIT pour une déclaration d'assignations spatiales**.

Le choix de la France peut être lié au fait que **les procédures de déclaration sont bien connues et suivies par l'ANFR** ou que **l'ANFR défend efficacement les assignations auprès de l'UIT**. Les opérateurs peuvent aussi être sensibles **au coût modique de la redevance** pour une autorisation d'utilisation d'une assignation spatiale, **20 000 euros**, comparé à d'autres pays.

Par ailleurs, **la France peut être mieux placée que d'autres pays pour demander des assignations** : par exemple, Hispasat, qui souhaitait couvrir l'Amérique Latine, avait sollicité l'ANFR puisque **la Guyane donne à la France des droits dans cette région**.

L'exploitation d'une assignation de fréquence à un système satellitaire, déclarée par la France à l'UIT, est ensuite soumise à **l'autorisation du ministre chargé des communications électroniques**, après avis des autorités affectataires des fréquences radioélectriques concernées.

L'octroi de l'autorisation est subordonné à **la justification par le demandeur de sa capacité à contrôler l'émission de l'ensemble des stations radioélectriques**, y compris les stations terriennes, **utilisant l'assignation de fréquence**, ainsi qu'au versement à l'ANFR **d'une redevance correspondant aux coûts de traitement du dossier déclaré à l'UIT**.

L'autorisation d'assignation de fréquence relative à un système satellitaire peut être refusée dans les cas suivants :

- pour **la sauvegarde de l'ordre public**, **les besoins de la défense** ou ceux **de la sécurité publique** ;
- lorsque **la demande n'est pas compatible**, soit avec **les engagements souscrits par la France dans le domaine des radiocommunications**, soit avec **les utilisations existantes ou prévisibles de bandes de fréquences**, soit avec **d'autres demandes d'autorisation permettant une meilleure gestion du spectre des fréquences** ;
- lorsque **la demande a des incidences sur les droits attachés aux assignations de fréquence antérieurement déclarées par la France** à l'Union internationale des télécommunications ;
- lorsque **le demandeur a fait l'objet d'une des sanctions** prévues au III de l'article L. 97-2 ou à l'article L. 97-3.

La France gère actuellement **603 dossiers fréquences satellites à l'UIT**, pour **les opérateurs gouvernementaux** (CNES, Ministère des Armées), **les organisations internationales** (Agence Spatiale Européenne, Eutelsat OIG, le groupe de pays du système Galileo, et l'Union Européenne pour une partie de la constellation souveraine européenne Iris²), et **les opérateurs privés français**.

Un dossier fréquences satellite, appelé *filing*, permet de réserver des fréquences pour **une durée maximale de 7 ans**. Les *filings* notifiés et mis en service avant la fin des 7 ans obtiennent **une reconnaissance et protection internationale**. Un *filing* peut représenter **un satellite unique** (géostationnaire ou non-géostationnaire), ou **un ensemble cohérent de satellites** (constellation).

2) Les obligations auxquelles doit se conformer le titulaire d'une autorisation d'assignation de fréquence relative à un système satellitaire

Le titulaire d'une autorisation doit **respecter les spécifications techniques** notifiées par la France à l'UIT ainsi que, le cas échéant, **les accords de coordination** conclus avec d'autres États membres de l'UIT ou avec d'autres exploitants d'assignations de fréquence déclarées par la France à l'UIT, y compris **les accords postérieurs à la délivrance de l'autorisation**.

Le titulaire doit assurer, de façon permanente, **le contrôle de l'émission de l'ensemble des stations radioélectriques**, y compris les stations terriennes, utilisant l'assignation de fréquence.

Le titulaire de l'autorisation doit **apporter son concours à l'administration** pour la mise en œuvre des dispositions du règlement des radiocommunications (RR).

À la demande du ministre chargé des communications électroniques, le titulaire de l'autorisation doit **faire cesser tout brouillage préjudiciable occasionné par le système satellitaire** ayant fait l'objet de l'autorisation, dans les cas prévus par le règlement des radiocommunications.

Les obligations que le présent article met à la charge du titulaire de l'autorisation s'appliquent également **aux stations radioélectriques faisant l'objet de l'autorisation qui sont détenues, installées ou exploitées par des tiers ou qui sont situées hors de France**.

L'autorisation est **accordée à titre personnel** et **ne peut être cédée à un tiers**. Elle **ne peut faire l'objet d'un transfert qu'après accord de l'autorité administrative**.

L'autorisation devient **caduque** si l'exploitation **se révèle incompatible avec les accords de coordination postérieurs à la délivrance de l'autorisation**.

3) L'existence d'un dispositif de sanctions

Le III de l'article L. 97-2 prévoit que **lorsque le titulaire de l'autorisation** prévue au I **ne respecte pas les obligations** qui lui sont imposées par les textes législatifs ou réglementaires, le ministre chargé des communications électroniques **le met en demeure** de s'y conformer dans un délai déterminé.

Si le titulaire ne donne pas suite à la mise en demeure qui lui a été adressée, le ministre chargé des communications électroniques peut prononcer à son encontre **l'une des sanctions** prévues au 2° de l'article L. 36-11. La procédure prévue aux 2° et 5° de l'article L. 36-11 est applicable. Il peut, en outre, décider **d'interrompre la procédure engagée par la France auprès de l'UIT**.

4) Autres autorisations susceptibles d'être nécessaires

Le IV de l'article 97-2 prévoit que l'obtention de l'autorisation prévue au I ne dispense pas, le cas échéant, **des autres autorisations prévues par les lois et règlements en vigueur**, notamment de celles concernant la fourniture de services de radio ou de télévision sur le territoire français prévues par la loi n° 86-1067 du 30 septembre 1986 précitée.

5) Cas dans lesquels les dispositions de l'article L. 97-2 ne sont pas applicables

Le V prévoit que les dispositions de l'article L. 97-2 ne sont pas applicables :

- **lorsque l'assignation de fréquence est utilisée par une administration pour ses propres besoins** dans une bande de fréquences dont elle est affectataire, en application de l'article 21 de la loi n° 86-1067 du 30 septembre 1986 précitée ;

- **lorsque la France a agi auprès de l'UIT, en sa qualité d'administration notificatrice, au nom d'un groupe d'États membres de l'Union internationale des télécommunications**.

6) Mesures réglementaires d'application

Le VI de l'article L. 97-2 dispose qu'un décret en Conseil d'État précise :

- la procédure selon laquelle **les autorisations sont délivrées ou retirées** et selon laquelle **leur caducité est constatée** ;
- **la durée** et **les conditions de modification et de renouvellement de l'autorisation** ;
- **les conditions de mise en service du système satellitaire** ;
- **les modalités d'établissement et de recouvrement de la redevance** prévue au deuxième alinéa du 2 du I.

II. Le dispositif envisagé – une volonté de conditionner le recours à l'ANFR à un véritable intérêt pour l'économie française et à une absence de compromission de la sécurité nationale

De plus en plus d'opérateurs veulent **déployer des constellations en orbite basse** et souhaitent obtenir, **pour garantir la qualité de leur service, la possibilité d'exploiter des bandes de fréquences sans risques de brouillage**.

Dans ce contexte, **ces opérateurs cherchent à déterminer l'État** qui sera **le plus en mesure** de leur obtenir auprès de l'UIT **une autorisation d'exploitation d'assignation permettant d'éviter ces risques de brouillage,** en défendant les droits dudit opérateurs vis à vis des autres utilisateurs du spectre au sein de l'UIT.

Or, **l'Agence nationale des fréquences (ANFR) française**, très impliquée dans les travaux de l'UIT, est **particulièrement reconnue pour le sérieux des analyses techniques qu'elle produit**, notamment en ce qui concerne **les conditions de coexistence entre systèmes satellitaires**.

En conséquence, **de nombreux acteurs internationaux** font le choix de **s'adresser à la France** afin de bénéficier **d'une autorisation d'exploiter une assignation de fréquence déposée auprès de l'UIT**.

Si cette situation témoigne de **l'excellence de l'expertise française dans ce domaine**, il parait néanmoins indispensable **de s'assurer que les acteurs privés qui bénéficient de ce savoir-faire français en matière de gestion des fréquences ne nuisent pas aux intérêts de la sécurité et de la défense nationale et contribuent au développement de l'économie française**.

Au-delà de cette nécessité de **s'assurer que l'expertise de l'ANFR est toujours utilisée à bon escient**, il est essentiel que **la France puisse valoriser au mieux son patrimoine en matière de fréquence**, qui est **le troisième plus**

important au niveau mondial, en particulier dans les bandes de fréquences Ku, Ka et Qv.

Or **cette valorisation demeure insuffisante** car la marge de manœuvre dont dispose l'ANFR en vertu des dispositions actuelles de l'article L.97-2 du code des postes et communications électroniques **quant à la décision d'autoriser ou non un acteur à utiliser ces ressources est particulièrement réduite**.

L'objet du présent article 42 consiste par conséquent à modifier l'article L. 97-2 dudit code est donc principalement **d'étendre la marge de manœuvre de l'État avant, durant et après le processus d'autorisation**.

1) <u>La protection des intérêts économiques et des intérêts de la sécurité nationale</u>

La nouvelle rédaction du 1 du I de l'article L. 97-2 du CPCE prévoit toujours que **toute demande d'assignation de fréquence relative à un système satellitaire est adressée à l'Agence nationale des fréquences (ANFR)** et que celle-ci déclare, au nom de la France, **l'assignation de fréquence correspondante à l'Union internationale des télécommunications (UIT)** et engage **la procédure prévue par le règlement des radiocommunications (RR)**.

Si la réserve de la conformité au tableau national de répartition des bandes de fréquences ou aux stipulations des instruments de l'UIT est maintenue, l'article 42 du présent projet de loi **ajoute deux autres réserves possibles, susceptibles de ne pas entrainer de déclaration de l'assignation de fréquence par l'ANFR à l'UIT**, à savoir :

- **l'existence d'un intérêt économique** ou **d'un intérêt pour la défense nationale** justifiant que la déclaration soit effectuée au nom de la France

De fait, **l'utilisation des moyens administratifs français** doit s'accompagner **d'un alignement de l'opérateur sur les intérêts français**. Certains opérateurs **recherchent en effet la juridiction la plus favorable, sans établir de lien direct avec le pays choisi**. Un exemple récent a été donné par l'opérateur ABS qui exploite actuellement des fréquences déclarées par la Fédération de Russie à l'UIT. ABS, pourtant concurrent direct d'Eutelsat, cherche à changer de pavillon et s'est renseigné sur les conditions pour devenir opérateur français.

- que **les assignations soumises ne soient pas de nature à compromettre les intérêts de la sécurité nationale** et **le respect par la France de ses engagements internationaux**.

Ce critère existe déjà en France au moment de la délivrance de l'autorisation au 2 du I de l'article 97-2.

Pourtant, chaque fois que cela est possible, il est préférable de **vérifier ces critères en amont** car il est trop tard au stade de l'autorisation pour

modifier les fréquences ou les caractéristiques techniques en cas de problème. Des États, tels que les Etats-Unis ou la Fédération de Russie, procèdent d'ailleurs à cette **analyse au début du processus** (demande d'assignations de fréquences) plutôt qu'à la fin (demande d'autorisation d'exploitation).

2) La mise en place d'un critère de rattachement juridique à la France et un élargissement des motifs de refus d'autorisation

Au 2 du I de l'article 97-2 relatif aux critères à respecter pour obtenir l'autorisation d'exploiter une assignation de fréquence à un système satellitaire, il est ajouté **une nouvelle condition**, à savoir que **l'autorisation est octroyée à une entité de droit français ou à un établissement immatriculé au registre du commerce et des sociétés en France**.

Selon l'ANFR, entendue par votre rapporteur, il s'agit de s'assurer que **certains droits sur des assignations françaises stratégiques** ne puissent **pas passer sous le contrôle de sociétés étrangères grâce aux procédures encadrant les investissements étrangers**.

Le problème s'est posé pour les assignations spatiales de *OneWeb* dont une partie repose sur des droits français bénéficiant d'une priorité règlementaire et qui était détenues par une filiale maltaise de *OneWeb*. **Aucun moyen juridique n'était disponible à l'époque pour éviter un rachat ultérieur de cette filiale par une société non européenne**.

Par ailleurs, les sanctions administratives prises par le ministre ne sont pas exécutoires dans les autres États, en l'absence de dispositions européennes sur l'exécution de telles décisions.

Dans la liste des motifs pouvant conduire à un refus de l'autorisation, sont donc rajoutés :

- **le respect par la France de ses engagements internationaux** ;
- **lorsque le demandeur ne peut démontrer qu'un intérêt économique s'attache, pour la France, à l'autorisation** ;
- **lorsque le demandeur est dans l'incapacité technique ou financière de faire face durablement aux obligations qui sont les siennes une fois l'autorisation obtenue**.

Enfin un dernier alinéa est ajouté au I pour prévoir que l'autorisation d'exploiter une assignation de fréquence à un système satellitaire peut être assortie, le cas échéant, de conditions visant à assurer que les activités prévues dans le cadre de l'exploitation de l'assignation autorisée **ne porteront pas atteinte aux intérêts de la sécurité et de la défense nationale** ou **au respect par la France de ses engagements internationaux**.

3) Une refonte complète du système de sanctions

Le présent article 42 réécrit ensuite entièrement le second alinéa du III de l'article L. 97-2 pour prévoir **un dispositif de sanctions plus efficace**.

Il prévoit que lorsque le titulaire de l'autorisation **ne se conforme pas**, dans les délais fixés, **à la mise en demeure** qui lui a été adressée, **le ministre chargé des communications électroniques peut lui notifier les griefs**.

Après que l'intéressé **a reçu la notification des giefs** et a été mis à même de consulter le dossier et de présenter ses observations écrites, le ministre chargé des communications électroniques procède, avant de prononcer une sanction, à **son audition selon une procédure contradictoire**.

Le ministre chargé des communications électroniques peut, en outre, **entendre toute personne dont l'audition lui paraît utile**.

Il peut prononcer, à l'encontre du titulaire de l'autorisation d'exploiter une assignation de fréquence, une des sanctions suivantes :

- **la suspension**, totale ou partielle, pour un mois au plus, **de l'autorisation**, **la réduction de sa durée**, dans la limite d'une année, **ou son retrait** ;

– une sanction pécuniaire dont le montant **est proportionné à la gravité du manquement** et aux avantages qui en sont retirés, **sans pouvoir excéder 3 % du chiffre d'affaires** hors taxes du dernier exercice clos, ou **5 % de celui-ci** en cas **de nouvelle violation de la même obligation**. À défaut d'activité permettant de déterminer ce plafond, le montant de la sanction ne peut excéder **150 000 euros**, **ou 375 000 euros en cas de nouvelle violation de la même obligation** ;

– l'interruption de la procédure engagée par la France auprès de l'Union internationale des télécommunications (UIT).

Lorsque le manquement est constitutif d'une infraction pénale, le montant total des sanctions prononcées ne peut excéder **le montant de la sanction encourue le plus élevé**.

Lorsque le ministre chargé des communications électroniques a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué sur les mêmes faits ou des faits connexes, ce dernier peut ordonner **que la sanction pécuniaire s'impute sur l'amende qu'il prononce**.

Les sanctions pécuniaires sont **recouvrées comme les créances de l'État étrangères à l'impôt et au domaine**.

Les décisions du ministre chargé des communications électroniques **sont motivées et notifiées à l'intéressé**. Elles peuvent être **rendues publiques** dans les publications, journaux ou services de communication au public par voie électronique choisis par lui, dans un format et pour une durée proportionnée à la sanction infligée. Elles peuvent **faire l'objet d'un recours de pleine juridiction**.

4) Mesures d'application

Le présent article 42 réécrit entièrement le VI de l'article L. 97-2 relatif au décret en Conseil d'État fixant les modalités d'application de cet article.

À toutes les modalités que le décret en Conseil d'État prévu par la version actuelle de l'article L. 97-2 prévoyait, il en rajoute deux autres, à savoir :

- les conditions dans lesquelles l'ANFR déclare, au nom de la France, les assignations de fréquence à l'UIT ;
- les conditions dont les autorisations d'exploitation peuvent être assorties ;
- la durée et les conditions de modification et de renouvellement de l'autorisation ;
- les modalités des procédures de mise en demeure et de sanctions prévues dans la nouvelle rédaction du III.

Il est enfin prévu que les dispositions du présent article 42 s'appliquent à compter de l'entrée en vigueur du décret en Conseil d'État prévu au VI et au plus tard le 31 décembre 2025.

III. La position de la commission – les entreprises doivent être en mesure de faire valoir l'existence d'un intérêt économique ou d'un intérêt pour la défense nationale justifiant qu'une demande d'autorisation d'assignation de fréquence relative à un système satellitaire soit effectuée au nom de la France

Comme rappelé *supra*, **de nombreux acteurs internationaux** font le choix de **s'adresser à la France** afin de bénéficier **d'une autorisation d'exploiter une assignation de fréquence déposée auprès de l'UIT**, car l'ANFR est très reconnue pour sa capacité à les obtenir.

Si cette situation témoigne de **l'excellence de l'expertise française dans ce domaine**, il parait néanmoins indispensable **de s'assurer que les acteurs privés qui bénéficient de ce savoir-faire français en matière de gestion des fréquences ne nuisent pas aux intérêts de la sécurité et de la défense nationale et contribuent au développement de l'économie française**.

Au-delà de cette nécessité de **s'assurer que l'expertise de l'ANFR est toujours utilisée à bon escient**, il est essentiel que **la France puisse valoriser au mieux son patrimoine en matière de fréquence**, qui est **le troisième plus important au niveau mondial**, en particulier dans les bandes de fréquences Ku, Ka et Qv.

C'est pourquoi les évolutions portées par le présent article 42 et visant à **accorder plus de marges de manœuvres à l'ANFR** et au ministre chargé des communications électroniques **avant, durant et après le processus d'autorisation d'assignation de fréquence relative à un système satellitaire** sont particulièrement bienvenues.

Le savoir-faire de l'ANFR doit en effet bénéficier **non à des entreprises étrangères sans liens avec la France** et **uniquement à la recherche**

de la juridiction la plus favorable à leurs intérêts (pratique dite du « *forum shipping* »), mais à **des entreprises qui sont en mesure de faire valoir l'existence d'un intérêt économique ou d'un intérêt pour la défense nationale justifiant que la déclaration soit effectuée au nom de la France**.

Il est en outre primordial que **les assignations de fréquence relative à un système satellitaire** soumises à l'UIT ne soient **pas de nature à compromettre les intérêts de la sécurité nationale** et **le respect par la France de ses engagements internationaux**.

En 2023, l'ANFR a traité **55 demandes de dépôts d'assignations**. Elle estime que de l'ordre de **trois cas par an** seraient susceptibles **de faire l'objet d'un contrôle approfondi** au titre de ces nouvelles dispositions. Il s'agira donc **d'un changement limité en termes quantitatifs**, mais qui, dans des cas d'espèce, pourrait revêtir **une réelle importance**.

La refonte du processus de sanctions ne posant par ailleurs pas de difficultés particulières, la commission spéciale a adopté l'article 42 uniquement avec un amendement rédactionnel COM 125 du rapporteur Patrick Chaize.

La commission a adopté l'article ainsi modifié.

TITRE II
CYBERSÉCURITÉ

CHAPITRE IER
DE L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Article 43 A

Désignation de la Banque de France et de l'Autorité de contrôle prudentiel et de résolution comme autorités compétentes dans le cas où une entité financière est assujettie à plusieurs autorités de supervision

Le présent article prévoit de désigner la Banque de France et l'Autorité de contrôle prudentiel et de régulation (ACPR) comme seules autorités compétentes pour exercer les fonctions et missions prévues par le règlement « DORA » en matière de déclaration des incidents majeurs liés aux technologies de l'information et de la communication (TIC) et de notification volontaire des cybermenaces importantes, respectivement pour les dépositaires centraux et pour les personnes relevant, dans le secteur de la banque, des services de paiement et des services d'investissement, de la compétence de l'ACPR, à l'exception des entreprises de marché.

La commission a adopté cet article additionnel.

I. LE DROIT EXISTANT : L'ARTICLE 19 DU RÈGLEMENT « DORA » PRÉVOIT QUE LES ÉTATS MEMBRES DÉSIGNENT, POUR LES ENTITÉS FINANCIÈRES SOUMISES À LA SURVEILLANCE DE PLUSIEURS AUTORITÉS NATIONALES, UNE SEULE AUTORITÉ POUR RECEVOIR CERTAINES DÉCLARATIONS ET NOTIFICATIONS

L'article 19 du règlement (UE) 2022/2554 du 14 décembre 2022, dit « DORA »[1], prévoit que les entités financières déclarent à l'autorité compétente pertinente les incidents majeurs liés aux technologies de l'information et de la communication (TIC). Il dispose également que, lorsqu'une entité financière est soumise à la surveillance de plusieurs autorités, les États membres désignent une seule autorité compétente en tant

[1] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

qu'autorité compétente concernée chargée d'exercer les fonctions et missions prévues à l'article 19.

Ces missions résident dans la réception de notification initiale et de rapports à la suite d'un incident majeur, la réception des notifications à titre volontaire des cybermenaces lorsque les entités estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients, et la communication de détails sur l'incident majeur aux superviseurs de niveau européen.

II. LE DISPOSITIF PROPOSÉ : ÉVITER LE RISQUE DE DOUBLE ASSUJETTISSEMENT ENTRE « DORA » ET « NIS 2 »

Le présent article, résultant d'un amendement déposé par le rapporteur Michel Canévet, a pour objet de répondre à cette exigence prévue par le règlement en désignant la Banque de France et l'Autorité de contrôle prudentiel et de régulation (ACPR) comme seules autorités compétentes pour exercer les fonctions et missions prévues par le règlement « DORA » en matière de déclaration des incidents majeurs liés aux technologies de l'information et de la communication (TIC) et de notification volontaire des cybermenaces importantes, respectivement pour les dépositaires centraux et pour les personnes relevant, dans le secteur de la banque, des services de paiement et des services d'investissement, de la compétence de l'ACPR, à l'exception des entreprises de marché. Il crée pour ce faire un article L. 142-10 au sein du code des marchés financiers, dans la partie relative aux missions de la Banque de France, et un article L. 612-24-1 dans la partie relative à celles de l'ACPR.

La désignation d'un « guichet unique » constitue une mesure de simplification qui, sans préjudice des échanges d'informations entre les services administratifs compétents, réduit la charge administrative des entreprises qui constituent par suite un unique dossier de déclaration ou de notification.

Décision de la commission : la commission a adopté l'article additionnel.

Article 43

Modification de la définition des prestataires de services techniques

Le présent article prévoit de modifier la définition des services fournis par les prestataires de services techniques à l'appui des services de paiement. L'expression « et de la communication » est ajoutée aux technologies de l'information, pour se mettre en conformité avec l'article 7 de la directive DORA.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : LA DÉFINITION DES SERVICES TECHNIQUES À L'APPUI DES SERVICES DE PAIEMENT EST ISSUE DE LA TRANSPOSITION DE LA 2ÈME DIRECTIVE SUR LES SERVICES DE PAIEMENT (DSP2) DE 2015

L'article L. 314-1 du code monétaire et financier (CMF) définit les **services fournis par les prestataires de services techniques** pour appuyer la fourniture de services de paiement. Ces prestataires de services techniques sont des acteurs **fournissant des services support à l'exécution d'opérations de paiement**.

La définition de ces services techniques est issue de la transposition de l'article 3 de la **directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015** concernant les services de paiement dans le marché intérieur (dite **« DSP2 »**)[1]. La DSP2 effectue une distinction entre les **services de paiement**, limitativement énumérées à son annexe I et dont la fourniture requiert un agrément, et les **services techniques**, qui ne requièrent pas d'agrément spécifique. La directive précise que les services fournis par les prestataires de services techniques n'entrent « **à aucun moment, en possession des fonds à transférer** »[2].

Le 7° de l'article L. 314-1 du CMF reprend la définition donnée par l'article 3 de la DSP2. Il précise ainsi que les **services techniques** à l'appui de la fourniture de services de paiement consistent « *notamment dans le traitement et l'enregistrement des données, les services de protection de la confiance de la vie privée, l'authentification des données et des entités, les technologies de l'information*

[1] *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE. L'article 3 de la DSP2 a été transposée dans le droit national par l'article 17 de l'ordonnance n°2017-1433 du 4 octobre 2017.*

[2] *Paragraphe j) de l'article 3 de la DSP2.*

et la fourniture de réseaux de communication, ainsi que la fourniture et la maintenance des terminaux et dispositifs utilisés aux fins des services de paiement, à l'exception des services d'initiation de paiement et des services d'information sur les comptes ».

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI ACTUALISE LA DÉFINITION DES SERVICES TECHNIQUES À L'APPUI DES SERVICES DE PAIEMENT POUR PERMETTRE LA TRANSPOSITION DE LA DIRECTIVE DORA

L'article 7 (1) de la directive DORA[1] modifie la définition des services fournis par les prestataires de services techniques qui figure à l'article 3 de la DSP2. Le paragraphe j) de l'article 3 de la DSP2 est amendé pour y inclure les services de fourniture des « ***technologies de l'information et de la communication*** » (TIC), dont les risques sont désormais uniformément couverts par le règlement DORA.

L'article 43 du projet de loi transpose dans le code monétaire et financier l'article 7 (1) de la directive DORA. **Le 7° de l'article L. 314-1 du code monétaire et financier**, qui dresse une liste non limitative des services fournis par les prestataires de services techniques à l'appui des services de paiement, est modifié en ajoutant « ***et de la communication*** » à la mention des technologies de l'information.

Cette modification a pour but **d'aligner la terminologie contenue dans le droit français sur celle adoptée par la règlementation DORA**. La mention des « technologies de l'information et de la communication » (TIC) est ainsi intégrée dans la liste des services fournis par les prestataires de services techniques à l'appui des services de paiement.

III. LA POSITION DE LA COMMISSION : UNE ACTUALISATION NÉCESSAIRE DE LA DÉFINITION DES SERVICES TECHNIQUES À L'APPUI DES SERVICES DE PAIEMENT

L'expression « **technologies de l'information et de la communication** » (TIC) est une terminologie aujourd'hui largement reprise par les acteurs fournissant des **services support à l'exécution des opérations de paiement**. La directive DORA actualise donc la définition des services fournis par les prestataires de services techniques à l'appui des services de paiement, qui figurait dans la DSP2.

---

[1] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier*

Le présent article permet de **transposer la définition de ces services techniques donnée par l'article 7 (1) de la directive DORA** et d'harmoniser ainsi la définition française sur la **terminologie retenue au niveau européen.**

Décision de la commission : la commission a adopté l'article sans modification

Article 44

Maintien de la résilience opérationnelle des gestionnaires de plateformes de négociation

Le présent article vise à transposer dans le droit interne le quatrième paragraphe de l'article 6 de la directive « DORA ».

Ce faisant, il impose aux gestionnaires de plates-formes de négociation de mettre en place et maintenir leur résilience opérationnelle conformément aux exigences fixées au chapitre II du règlement « DORA », lequel impose aux entités financières le respect nombreuses obligations en termes de gouvernance, de contrôle interne et de gestion du risque ainsi que la mise en place d'une gouvernance et d'un cadre de gestion du risque cyber, ainsi que de différentes mesures techniques destinées à se prémunir face au risque cyber, à en atténuer les conséquences et en tirer des enseignements.

Par ailleurs, il prévoit que les mécanismes assurant la continuité des activités en cas de défaillance imprévue de ses systèmes de négociations, et qui doivent être mises en place par le gestionnaire, incluent une politique et des plans en matière de continuité des activités et des plans de réponse et de rétablissement des technologies de l'information et de la communication, mis en place conformément à l'article 11 du règlement « DORA », lequel impose aux entités financières, d'une part, de se doter d'une politique de continuité des activités visant notamment à résoudre les incidents, estimer leur impact et définir les mesures adaptés de communication et de gestion des crises, et, d'autre part, de mettre en œuvre des plans de réponse et de rétablissement des TIC, qui font l'objet de tests.

Enfin, il prévoit que les tests d'algorithmes auxquels doivent procéder, sur injonction des gestionnaires de plates-formes de négociation, les personnes utilisant des systèmes de négociation algorithmique, et les environnements de tests dont elles doivent disposer, s'inscrivent dans le cadre fixé par les chapitres II et IV du règlement « DORA », qui encadrent respectivement la gestion du risque lié aux technologies de l'information et de la communication et les tests de résilience opérationnelle numérique.

La commission a adopté cet article sans modification.

I. UN DÉCALAGE ENTRE LES DROITS INTERNE ET EUROPÉEN EN MATIÈRE D'OBLIGATION DE GESTION DES RISQUES CYBER PAR LES GESTIONNAIRES DE PLATES-FORMES DE NÉGOCIATION

A. LES GESTIONNAIRES DES PLATEFORMES DE NÉGOCIATION DOIVENT S'ASSURER DE LA RÉSILIENCE DES SYSTÈMES DE NÉGOCIATION QU'ILS EXPLOITENT

1. Les plates-formes de négociation regroupent les marchés réglementés, les systèmes multilatéraux de négociation et les systèmes organisés de négociation

L'article L. 420-1 du code monétaire et financier définit la plate-forme de négociation. Il constitue en ceci une transposition en droit français de la directive « MIF 2 »[1], et en particulier de son article 4.

Une plate-forme de négociation est donc un système multilatéral, défini par le code monétaire et financier comme « *un système ou un dispositif au sein duquel de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des instruments financiers peuvent interagir* », qui **peut prendre trois formes**[2] :

- un **marché réglementé** au sens de l'article L. 421-1, qui vise à aboutir à la conclusion de contrats portant sur les instruments financiers admis à la négociation. On compte en France trois marchés réglementés agréés : Euronext Paris SA, le Matif (marché à terme international de France) et le Monep (marché des options négociables de Paris) ;

- un **système multilatéral de négociation** au sens de l'article L. 424-1, qui vise à la conclusion de transactions sur des instruments financiers, qui compte au moins trois membres. On compte en France huit systèmes latéraux de négociation agréés (pour 14 codes d'identification de marché), dont Euronext Growth Paris et Euronext Access Paris ;

- un **système organisé de négociation** au sens de l'article L. 425-1, visant à conclure des transactions sur les titres de créance, les produits financiers structurés, les quotas carbones, des instruments dérivés (c'est-à-dire une valeur mobilière donnant le droit d'acquérir ou de vendre de telles valeurs mobilières ou donnant lieu à un règlement en espèce), ou des produits énergétiques de gros. On compte en France 10 systèmes organisés de négociation agréés.

2. Le droit interne relatif aux obligations des gestionnaires des plates-formes de négociation en matière de gestion du risque

---

[1] *Directive (UE) n° 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.*

[2] *Voir la liste des gestionnaires de plates-formes de négociation agréées sur le site de l'Autorité des marchés financiers sur sa page « Obtenir un agrément pour une plate-forme de négociation ».*

cyber est une transposition de la directive « MIF 2 » dans sa version de 2014

L'article 48 de la directive précitée dans sa version de 2014 prévoit en son paragraphe 1er que les États membres exigent d'un marché réglementé qu'il dispose de systèmes, de procédures et de mécanismes efficaces pour garantir que ses systèmes de négociation sont résilients, possèdent une capacité suffisante pour gérer les volumes les plus élevés d'ordres et de messages, sont en mesure d'assurer un processus de négociation ordonné en période de graves tensions sur les marchés, sont soumis à des **tests exhaustifs afin de confirmer que ces conditions sont réunies** et sont régis par des mécanismes de continuité des activités assurant le maintien de ses services en cas de défaillance de ses systèmes de négociation.

L'article L. 420-3 du code monétaire et financier, en son I, transpose ces dispositions et détermine ainsi les obligations du gestionnaire de la plate-forme de négociation en matière de risque cyber.

C'est à lui qu'il revient de mettre en place les **systèmes, des procédures et des mécanismes efficaces** mentionnés par l'article 48 de la directive, à ceci près que l'article vise un processus de négociation ordonné en période de tension sur les marchés, et non de « graves tensions ».

Il est également précisé que ces **systèmes de négociation sont soumis à des tests** afin de confirmer que ces conditions sont réunies dans des situations d'extrême volatilité des marchés, et que le gestionnaire met en place des mécanismes assurant la continuité des activités en cas de défaillance imprévue de ses systèmes de négociation. Le législateur français a ici utilisé sa **marge de manœuvre** en prévoyant que les systèmes financiers doivent surtout résister à des chocs importants et imprévus, là où le droit européen n'évoque pas « les situations d'extrême volatilité ».

L'article 48 régit également, en son paragraphe 6, le cadre de gestion du risque cyber des marchés réglementés en matière de trading algorithmique.

Il prévoit ainsi que les États membres exigent d'un **marché réglementé** qu'il dispose de systèmes, de procédures et de mécanismes efficaces, y compris qu'il **exige de ses membres ou de ses participants qu'ils procèdent à des essais appropriés d'algorithmes et mettent à disposition les environnements facilitant ces essais**. Le but est de garantir que les systèmes de trading algorithmique ne donnent pas naissance ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché, mais aussi de gérer ces conditions de négociation lorsqu'elles découlent de ces systèmes de trading algorithmique, y compris de systèmes permettant de limiter la proportion d'ordres non exécutés par rapport aux transactions susceptibles d'être introduites dans le système par un membre ou un participant, de ralentir le flux d'ordres si le système risque d'atteindre sa

capacité maximale ainsi que de limiter le pas minimal de cotation sur le marché et de veiller à son respect.

Transposant ces dispositions en droit interne, le III de l'article L. 420-3 du code monétaire et financier prévoit que le gestionnaire de la plate-forme de négociation exige des personnes qui les utilisent qu'elles « *procèdent à des tests appropriés d'algorithme et disposent d'environnements de tests* », afin de s'assurer que ces systèmes « *ne créent pas ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché* ». Les systèmes, procédure et mécanismes mis en place dans ce cadre doivent également permettre de « *gérer les conditions de négociation de nature à perturber le bon ordre du marché qui découlent de ces systèmes de négociation algorithmique* ».

Par ailleurs, selon le II, de l'article L. 420-3 du code monétaire et financier, le gestionnaire est également chargé de mettre en place des systèmes permettant de rejeter les ordres dépassant des seuils de volume ou les ordres erronés ainsi que de suspendre ou limiter temporairement la négociation en cas de fluctuation importante des prix. En ce cas, il notifie à l'Autorité des marchés financiers les paramètres de suspension de la négociation ainsi que tout changement de ceux-ci. Les IV et V de l'article déterminent enfin les obligations qui s'imposent au gestionnaire en matière d'accès électronique direct et de sécurité et d'authentification des moyens de transfert d'informations.

B. LA DIRECTIVE « DORA » A MODIFIÉ LA DIRECTIVE « MIF 2 » SANS QUE LE DROIT INTERNE N'Y AIT ENCORE ÉTÉ ADAPTÉ

L'article 6 de la directive (UE) 2022/2556 du 14 décembre 2022, dite « DORA »[1], en son quatrième paragraphe, modifie notamment les paragraphes 1 et 6 de l'article 48 de la directive « MIF 2 ».

Le paragraphe 1 de la directive « MIF 2 » prévoit désormais un renvoi spécifique à diverses dispositions du paquet « DORA » : les États membres exigent d'un marché réglementé qu'il mette en place et maintienne sa résilience opérationnelle conformément aux exigences fixées au chapitre II du règlement (UE) 2022/2554 du 14 décembre 2022, dit « DORA »[2] qui traite de la gestion du risque lié aux technologies de l'information et de la communication (TIC).

Par ailleurs, les mécanismes de continuité des activités qui régissent les systèmes de négociation incluent désormais une politique et des plans en

---

[1] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

matière de continuité des activités des TIC et des plans de réponse et de rétablissement des TIC mis en place conformément à l'article 11 du règlement « DORA », qui précise le contenu de cette politique et de ces plans.

Selon cet article, les entités financières doivent se doter d'une **politique de continuité des activités de TIC complète**, qui vise à garantir la continuité des fonctions critiques ou importantes (y compris lorsqu'elles sont externalisées), répondre aux incidents et les résoudre, activer des plans comportant des mesures d'endiguement et **prévenir tout dommage supplémentaire**, estimer les incidences, dommages et pertes préliminaires et enfin définir des mesures de communication et de gestion des crises. Cette politique de continuité suppose une analyse de l'incidence de graves perturbations sur leurs activités. Les entités financières doivent également mettre en œuvre des plans de réponse et de rétablissement des TIC. Ces plans (continuité, réponse et rétablissement, communication) font l'objet de tests, notamment en incluant des scénarios de cyberattaques et de basculement entre l'infrastructure de TIC principale et la capacité redondante, et de réexamens périodiques.

Le paragraphe 6 de la directive « MIF 2 » prévoit désormais que la mise à disposition, par les membres ou participant d'un marché réglementé, d'« environnements » facilitant les essais d'algorithmes, doit se faire « *conformément aux exigences fixées aux chapitres II et IV du règlement (UE) 2022/2554* », qui encadrent respectivement la gestion du risque lié aux TIC et les tests de résilience opérationnelle numérique.

Les chapitres II et IV du règlement « DORA »

Le chapitre II du règlement « DORA » traite de la gestion du risque lié aux TIC et encadre, en ce sens, la gouvernance et le contrôle interne des entités financières (article 5), leur impose un cadre de gestion du risque lié au TIC précis (article 6), définit les prérequis des systèmes, protocoles et outils destinés à atténuer et gérer le risque lié aux TIC (article 7) et impose aux entités financières d'identifier en leur sein l'ensemble des éléments liés au TIC (article 8). Par ailleurs, il impose aux entités financières la mise en place d'instruments de protection, de prévention du risque cyber (article 9), de détection (article 10), d'une politique de continuité des activités (article 11, cf infra), et de mesures de sauvegarde et de restauration des activités (article 12). Il exige des entités financières qu'elles analysent les cyberattaques qu'elles subissent pour en tirer les conséquences (article 13), mettent en place des plans de communication de crise (article 14). Il institue enfin un cadre simplifié de gestion du risque lié au TIC pour certains petits établissements financiers (article 16).

Le chapitre IV traite, quant à lui, des tests de résilience opérationnelle numérique : y sont notamment fixées les exigences générales applicables à la réalisation de ces tests, incluant en particulier la mise en œuvre d'un programme de tests (article 24), ainsi que les caractéristiques techniques de ces tests (article 25). Il prévoit que les entités financières importantes réalisent tous les trois ans au moins un test de pénétration fondé sur la menace, supposant potentiellement la participation des prestataires tiers et réalisés par des testeurs externes qui rendent compte à l'autorité de supervision des résultats (article 26) et qui doivent respecter certains critères (article 27).

Source : commission spéciale

Subsiste donc un **décalage entre le droit interne** qui résulte, au sein de l'article L. 420-3 du code monétaire et financier, des dispositions de la directive « MIF 2 » dans sa rédaction de 2014, **et le droit européen**, qui a permis à travers le paquet « DORA » adopté en 2022 de préciser et compléter le cadre de gestion du risque cyber sur les marchés réglementés.

II. LE DISPOSITIF PROPOSÉ : SOUMETTRE LES GESTIONNAIRES DES PLATES-FORMES DE NÉGOCIATION AU RESPECT DES EXIGENCES DE CYBERSÉCURITÉ INTRODUITES PAR LE PAQUET « DORA »

Le présent article modifie l'article L. 420-3 du code monétaire et financier en reprenant les dispositions introduites à l'article 48 de la directive « MIF 2 » par le quatrième paragraphe de l'article 6 de la directive « DORA ».

Ainsi, son **1°** modifie le I de l'article L. 420-3 de façon à prévoir que le gestionnaire de plate-forme de négociation met en place non pas « *des systèmes, des procédures et des mécanismes efficaces* » pour garantir la résilience des systèmes de négociation – ce qui se ferait sans référence aux exigences du règlement DORA –, mais met en place « *et maintient sa résilience opérationnelle conformément aux exigences fixées au chapitre II* » du règlement « DORA ». Le gestionnaire doit aussi être en mesure d'assurer un processus de négociation ordonné en période de « *graves tensions* » - et non de simples tensions – sur les marchés. Enfin, les tests auxquels sont soumis les systèmes de négociation doivent désormais être « exhaustifs », afin de confirmer que ces conditions (résilience, gestion de volumes élevés d'ordre et messages et processus de négociation ordonné en période de grave tension) soient réunies, et ce à tout moment, et plus uniquement « *dans des situations d'extrême volatilité des marchés* ».

Par ailleurs, les mécanismes assurant la continuité des activités en cas de défaillance imprévue de ses systèmes de négociations, et qui doivent être mises en place par le gestionnaire, incluent une politique et des plans en matière de continuité des activités liées aux TIC et des plans de réponse et de rétablissement des TIC mis en place conformément à l'article 11 du règlement « DORA ».

Le **2°** du présent article modifie le III de l'article L. 420-3 du code monétaire et financier et prévoit que les tests d'algorithmes auxquels doivent procéder, sur injonction des gestionnaires de plates-formes de négociation, les personnes utilisant des systèmes de négociation algorithmique, et les environnements de tests dont elles doivent disposer, s'inscrivent dans le cadre fixé par les **chapitres II et IV du règlement « DORA ».** Il procède également à des modifications d'ordre rédactionnel.

III. LA POSITION DE LA COMMISSION : UNE MODIFICATION NÉCESSAIRE POUR TRANSPOSER LE DROIT EUROPÉEN ET ASSURER UNE MEILLEURE RÉSILIENCE DES PLATES-FORMES DE NÉGOCIATION

Le présent article consistant en une reprise à l'identique de la rédaction adoptée à l'article 6 de la directive « DORA », elle constitue une transposition limitée à l'essentielle du droit européen. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1]. Elle doit permettre d'assurer une meilleure résilience du secteur financier, à travers une meilleure gestion du risque lié au TIC, la notification des incidents majeurs aux autorités compétentes, et la mise en place de tests de résilience opérationnelle numérique.

Si le simple ajout de références aux chapitres du règlement « DORA » est d'une faible portée juridique dans la mesure où ce règlement est d'application directe, il permet une meilleure lisibilité du droit et reflète de façon fidèle la rédaction de la directive.

Décision de la commission : la commission a adopté l'article sans modification.

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 45

Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché

Le présent article vise à transposer dans le droit interne le troisième paragraphe de l'article 6 de la directive « DORA ».

Ce faisant, il prévoit que les entreprises de marché doivent disposer en permanence des moyens, d'une organisation et de procédures de suivi adéquats permettant de gérer les risques auxquels elle est exposée, y compris les risques liés aux technologies de l'information (TIC) et de la communication conformément au chapitre II du règlement « DORA » relatif à la gestion du risque lié aux TIC.

La commission a adopté l'article 45 modifié par un amendement rédactionnel du rapporteur.

I. LE DROIT INTERNE PRÉVOIT DÉJÀ QUE LES ENTREPRISES DE MARCHÉ DOIVENT POUVOIR IDENTIFIER LES RISQUES COMPROMETTANT LE FONCTIONNEMENT DU MARCHÉ RÉGLEMENTÉ QU'ELLES GÈRENT ET GARANTIR LA VIABILITÉ DES SYSTÈMES DESTINÉS À FAIRE FACE AUX ÉVENTUELS DYSFONCTIONNEMENTS, SANS POUR AUTANT SATISFAIRE LES CRITÈRES PRÉVUS PAR LE PAQUET « DORA »

Aux termes de l'article L. 421-2 du code monétaire et financier, l'entreprise de marché est une société de droit privé, empruntant la forme d'une société commerciale, dont l'activité principale consiste en la gestion, c'est-à-dire principalement **l'organisation et l'exploitation**, d'un marché réglementé.

En France, la principale entreprise de marché opérant sur le secteur est la société **NYSE Euronext**, vaste entité gérant les marchés Euronext de Paris, Amsterdam, Bruxelles, Lisbonne, et allié avec New York. D'autres entreprises de ce type peuvent être identifiées : Nasdaq, qui gère le marché américain éponyme ou le marché de Boston et de Philadelphie, Deutsche Börse AG (Francfort) ou encore London Stock Exchange (qui gère, outre le principal marché de Londres, celui de Milan).

En plus de ses missions de contrôle des membres du marché réglementé et de surveillance des transactions destinée à détecter tout manquement, **l'entreprise de marché,** aux termes de l'article L. 421-11 du code monétaire et financier, **prend notamment les dispositions nécessaires en vue de :**

- disposer en permanence des moyens, d'une organisation et de procédures de suivi adéquats permettant d'identifier les risques significatifs de nature à compromettre le bon fonctionnement du marché règlementé qu'elle gère et prendre les mesures appropriées pour atténuer ces risques (2. du I) ;

- garantir le bon fonctionnement des systèmes techniques de négociation et disposer notamment de procédures d'urgence destinées à faire face aux éventuels dysfonctionnements (4. du I).

Selon l'article L. 421-4 du code monétaire et financier, l'Autorité des marchés financiers (AMF), qui propose au ministre de l'économie la reconnaissance de la qualité de marché réglementé, consulte l'Autorité de contrôle prudentiel et de résolution (ACPR) sur les mesures prévues par l'entreprise de marché pour se conformer à ces obligations.

L'article L. 421-11, en confiant à l'entreprise de marché le rôle de gestion des risques pesant sur les marchés réglementés, assure ainsi la transposition de l'article 47 de la directive « MIF 2 » dans sa rédaction du 15 mai 2014. Celui-ci prévoit que les États membres exigent notamment des marchés réglementés qu'ils soient adéquatement équipés pour gérer les risques auxquels ils sont exposés, qu'ils mettent en œuvre des dispositifs et des systèmes appropriés leur permettant d'identifier tous les risques significatifs pouvant compromettre leur bon fonctionnement et qu'ils instaurent des mesures effectives pour atténuer ces risques (b du I), ainsi que des dispositifs propres à garantir la bonne gestion des opérations techniques des systèmes et notamment des procédures d'urgence efficaces pour faire face aux dysfonctionnements éventuels des systèmes de négociation (c du I).

Or l'article 6 de la directive (UE) 2022/2556 du 14 décembre 2022, dite « DORA »[1], en son troisième paragraphe, modifie ces dispositions pour raccrocher au règlement « DORA » les mesures qui doivent s'imposer aux marchés réglementés pour gérer le risque cyber. Il procède à une suppression du c du I de l'article 47 de la directive MIF 2, et réécrit le b du I de sorte que les marchés réglementés doivent prévoir de gérer le risque TIC conformément au chapitre II du règlement (UE) 2022/2554 du 14 décembre 2022, dit « DORA »[2], lequel satisfait les conditions prévues par l'ancien c du I.

---

[1] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011. Pour plus de détails sur le chapitre II du règlement « DORA », voir le commentaire de l'article 44.*

II. LE DISPOSITIF PROPOSÉ : LA SOUMISSION DES ENTREPRISES DE MARCHÉS AUX EXIGENCES DE MOYENS ET D'ORGANISATION PRÉVUS PAR LE PAQUET « DORA » POUR ASSURER LEUR RÉSILIENCE FACE AU RISQUE CYBER

Le présent article prévoit de modifier l'article L. 421-11 du code monétaire et financier de façon **à intégrer dans le droit français les exigences prévues par l'article 47 de la directive « MIF 2 » dans sa rédaction issue de la directive « DORA ».**

Il modifie ainsi le 2 du I de l'article L. 421-11 pour prévoir que les entreprises de marché doivent disposer en permanence des moyens, d'une organisation et de procédures de suivi adéquats permettant de gérer les risques auxquels elle est exposée, y compris les risques liés aux technologies de l'information et de la communication conformément au chapitre II du règlement « DORA ». Il procède également, par parallélisme avec la nouvelle rédaction de l'article 47 de la directive « MIF 2 », à la suppression du 4 du I.

Il contient également des mesures de coordination avec ces dispositions, au sein de l'article L. 421-11 lui-même ainsi qu'à l'article L. 421-4.

III. LA POSITION DE LA COMMISSION : UNE ÉVOLUTION NÉCESSAIRE POUR RACCROCHER LA GESTION DU RISQUE CYBER PAR LES ENTREPRISES DE MARCHÉ AUX CRITÈRES PRÉVUS PAR LE RÈGLEMENT « DORA »

Le présent article constitue une **transposition nécessaire du droit européen en matière de gestion du risque cyber par les entreprises de marché**, dont la résilience face aux cyberattaques et, plus généralement, au risque « TIC » doit être assurée, leur rôle dans le fonctionnement d'une économie de marché étant incontournable. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

La commission spéciale a adopté un amendement rédactionnel COM-127 du rapporteur Michel Canévet.

Décision de la commission : la commission a adopté l'article ainsi modifié.

---

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 46

Références aux risques liés aux technologies de l'information et de la communication au sein des dispositifs de gestion des risques des établissements de crédit et des sociétés de financement

Le présent article prévoit d'actualiser le cadre de surveillance prudentielle applicable aux établissements de crédit et aux sociétés de financement en matière de risque opérationnel, pour garantir la prise en compte par les sociétés et les régulateurs concernés des risques spécifiques liés aux technologies de l'information et de la communication.

L'article prévoit à ce titre, en transposant les obligations prévues par la directive DORA, que les établissements de crédit sont tenus de mettre en place des instruments de détection et de gestion des risques liés aux technologies de l'information et de la communication et des risques mis en évidence par les tests de résilience opérationnelle numérique prévus par le règlement DORA. L'article étend l'application de cette mise à jour aux sociétés de financement pour maintenir l'équivalence de leurs obligations prudentielles par rapport au secteur bancaire

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : LES ÉTABLISSEMENTS DE CRÉDITS ET LES SOCIÉTÉS DE FINANCEMENT SONT SOUMIS À UN DISPOSITIF DE SURVEILLANCE PRUDENTIELLE EN APPLICATION DU DROIT DE L'UNION

A. LA DIRECTIVE SECTORIELLE « CRD » DU 26 JUIN 2013 FIXE, NOTAMMENT EN MATIÈRE DE RISQUE OPÉRATIONNEL, UN CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT

La directive 2013/36/UE du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement[1], ou directive « CRD »[2], est une directive sectorielle ayant pour objet de fixer au sein de l'Union européenne

[1] *Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.*

[2] *Capital Requirements Directive (CRD).*

un régime homogène en matière d'accès à l'activité des banques et à l'exercice de cette activité.

Adoptée dans le cadre d'un paquet législatif élaboré en réaction à la crise économique et financière de 2008, la directive CRD renforce le cadre de surveillance prudentielle applicable au secteur bancaire. À ce titre, elle fixe les principales règles applicables en matière de surveillance prudentielle des établissements de crédit par les autorités nationales compétentes et détermine les pouvoirs et outils de surveillance dont ces autorités disposent.

En particulier, en premier lieu, le 2 de l'article 85 de la directive CRD prévoit que les autorités compétentes[1] veillent à ce que les établissements de crédit disposent de « plans d'urgence et de poursuite de l'activité » dont l'objet est d'assurer la capacité des établissements à limiter leur perte et à poursuivre leur activité en cas de matérialisation d'un risque opérationnel.

En second lieu, le 1 de l'article 97 de la directive CRD prévoit que les autorités compétentes évaluent l'exposition des établissements de crédit à plusieurs catégories de risque en vue d'apprécier la couverture de ces risques par les établissements de crédit.

B. LE CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT, NOTAMMENT EN MATIÈRE DE RISQUE OPÉRATIONNEL, A ÉTÉ TRANSPOSÉ EN DROIT NATIONAL DANS LE CODE MONÉTAIRE ET FINANCIER

Le cadre européen de surveillance prudentielle applicable au secteur bancaire a notamment été transposé en droit national par l'ordonnance du 20 février 2014 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière[2].

En particulier, en matière de risque opérationnel, l'article L. 511-41-1 B du code monétaire et financier prévoit en premier lieu que les établissements de crédit et les sociétés de financement mettent en place des dispositifs, stratégies et procédure pour détecter et gérer le risque opérationnel (alinéa 2).

En second lieu, l'alinéa 5 du même article prévoit que les établissements de crédit et les sociétés de financement doivent établir des plans d'urgence et de poursuite de leur activité.

---

[1] *La répartition des compétences entre les autorités compétentes nationales (ACN) et la Banque centrale européenne (BCE) est fixée par le règlement (UE) n° 468/2014 de la banque centrale européenne du 16 avril 2014 (règlement-cadre MSU).*

[2] *Ordonnance n° 2014-158 du 20 février 2014 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière.*

C. LA DIRECTIVE « DORA » DU 14 DÉCEMBRE 2022 A MIS À JOUR LE CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT EN MATIÈRE DE RISQUE OPÉRATIONNEL POUR TENIR COMPTE DES RISQUES SPÉCIFIQUES LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

La directive (UE) 2022/2556 du 14 décembre 2022[1], ou « directive DORA »[2], prévoit plusieurs dispositions de mise à jour de la directive sectorielle CRD.

En particulier, l'article 4 de la directive DORA prévoit d'actualiser le cadre de surveillance prudentielle fixé par la directive CRD.

En premier lieu, le 2 de l'article 85 de la directive CRD est modifié pour prévoit expressément que les autorités compétentes veillent à ce que les établissements de crédit disposent, dans le cadre de leur politiques et plans d'urgence et de poursuite de l'activité, de politiques et plans en matière de continuité des activités de technologies de l'information et de la communication (TIC) et des plans de réponse et de rétablissement des TIC.

En second lieu, un d est ajouté au 1 de l'article 97 de la directive CRD pour prévoir l'évaluation par les autorités compétentes des risques opérationnels mis en évidence par des tests de résilience opérationnelle numérique prévus par le règlement (UE) 2022/2554 du 14 décembre 2022, ou « règlement DORA »[3].

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI TRANSPOSE DANS LE DROIT NATIONAL LA MISE À JOUR, EN MATIÈRE DE RISQUE OPÉRATIONNEL, DU CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT ET ÉTEND SON APPLICATION AUX SOCIÉTÉS DE FINANCEMENT

L'article 46 du projet de loi transpose la mise à jour du cadre prudentielle applicable aux établissements de crédit en matière de risque opérationnel et étend cette mise à jour aux sociétés de financement.

En premier lieu, l'article 46 prévoit la modification des deuxième et cinquième alinéas de l'article L. 511-41-1 B du code monétaire et financier pour prévoir, d'une part, que les stratégies de gestion des risques tiennent

---

[1] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Digital Operational Resilience Act.*

[3] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

spécifiquement compte des risques liés aux technologies de l'information et de la communication au sens du règlement DORA et des risques mis en évidence par les tests de résilience opérationnelle numérique prévus par le règlement DORA et, d'autre part, que les plans d'urgence et de poursuite de l'activité comprennent des plans de réponse et de rétablissement des technologies de l'information et de la communication.

En second lieu, en procédant à cette modification du cadre prudentiel applicable aux établissements de crédit, le projet de loi impose les mêmes obligations actualisées en matière de risque opérationnel aux sociétés de financement qui sont assujetties aux obligations fixées par l'article L. 511-41-1 B du code monétaire et financier.

III. LA POSITION DE LA COMMISSION : L'APPLICATION DU CADRE ACTUALISÉ DE SURVEILLANCE PRUDENTIELLE EN MATIÈRE DE RISQUE OPÉRATIONNEL AUX ÉTABLISSEMENTS DE CRÉDIT ET AUX SOCIÉTÉS DE FINANCEMENT RÉPOND À LA NÉCESSITÉ DE TRANSPOSER LE DROIT DE L'UNION ET DE MAINTENIR UN TRAITEMENT HOMOGÈNE ENTRE LES ÉTABLISSEMENTS DE CRÉDIT ET LES SOCIÉTÉS DE FINANCEMENT

A. L'ACTUALISATION DU CADRE PRUDENTIEL APPLICABLE EN MATIÈRE DE RISQUE OPÉRATIONNEL AUX ÉTABLISSEMENTS DE CRÉDIT RÉSULTE DE L'OBLIGATION CONSTITUTIONNELLE DE TRANSPOSITION DU DROIT DE L'UNION

La mise à jour des obligations applicables aux établissements de crédit en matière de risque opérationnel correspond à la transposition de la directive DORA en droit national par la modification du code monétaire et financier. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

B. L'EXTENSION DE LA MISE À JOUR DU CADRE PRUDENTIEL APPLICABLE EN MATIÈRE DE RISQUE OPÉRATIONNEL AUX SOCIÉTÉS DE FINANCEMENT EST LÉGITIME AU REGARD DE L'OBJECTIF DE MAINTIEN D'UN TRAITEMENT HOMOGÈNE ENTRE CES DEUX ACTIVITÉS

Les sociétés de financement, qui sont des sociétés qui exercent une activité professionnelle de crédit sans collecter des dépôts, sont soumis en

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

France à un cadre prudentiel équivalent au cadre applicable au secteur bancaire[1]. Si le droit de l'Union ne prévoit pas d'obligation d'inclure ces sociétés dans le champ d'application du cadre prudentiel applicable aux établissements de crédit défini par la directive CRD, les autorités françaises ont choisi depuis 2013 d'appliquer à ces sociétés, sauf pour certaines obligations spécifiques notamment en matière de liquidité et de levier, les mêmes obligations prudentielles que celles applicables au secteur bancaire.

Ce choix est fondé sur la volonté de permettre aux établissements de crédits de bénéficier d'un régime favorable pour leurs expositions sur les sociétés de financement dans le cadre du calcul déterminant leur respect des exigences de fonds propres applicables aux établissements de crédit.

En effet, l'article 119 du « règlement CRR »[2] du 26 juin 2013[3] prévoit que, dans le cadre du calcul des ratios de fonds propres soumis aux exigences prudentielles applicables aux établissements de crédit, les expositions sur les établissements financiers qui, sans entrer dans le champ du règlement, sont soumis à l'agrément et à la surveillance des autorités compétentes et respectent « des exigences prudentielles comparables » à celles applicables au secteur bancaire sont traitées comme des expositions sur les établissements de crédit.

Par suite, l'extension de la mise à jour du cadre prudentiel en matière de risque opérationnel est justifiée par le fait qu'elle permet de maintenir des exigences prudentielles homogènes entre les établissements de crédit et les sociétés de financement, ce qui permet de garantir le maintien d'un régime favorable pour les expositions sur les sociétés de financement dans le cadre du respect des exigences fixées par le règlement CRR.

Décision de la commission : la commission spéciale a adopté cet article sans modification.

[1] *En 2024, le nombre de sociétés de financement agréées en France était de 144.*
[2] *Capital Requirement Regulation.*
[3] *Règlement (UE) n ° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n ° 648/2012.*

Article 47

Références aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement

Le présent article prévoit de mettre à jour le cadre prudentiel applicable aux établissements de crédit relatif à l'obligation de mise en place un dispositif de gouvernance solide, notamment en matière de réseaux et de systèmes d'information.

L'article prévoit à ce titre, en transposant les obligations prévues par la directive DORA, que le dispositif de gouvernance des établissements de crédit doit comprendre des réseaux et des systèmes d'information gérés conformément au règlement DORA.

L'article étend l'application de cette mise à jour aux sociétés de financement pour maintenir l'équivalence de leurs obligations prudentielles par rapport au secteur bancaire. La portée de cette extension sera en tout état de cause modulée par le principe de proportionnalité du dispositif de gouvernance fixé au dernier alinéa de l'article L. 511-55 du code monétaire et financier.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : LES ÉTABLISSEMENTS DE CRÉDIT ET LES SOCIÉTÉS DE FINANCEMENT ONT L'OBLIGATION DE DISPOSER D'UN CADRE DE GOUVERNANCE SOLIDE EN APPLICATION DU DROIT DE L'UNION

A. LA DIRECTIVE SECTORIELLE « CRD » DU 26 JUIN 2013 FIXE, UN CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT

La directive 2013/36/UE du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement[1], ou directive « CRD »[2], est une directive sectorielle ayant pour objet de fixer au sein de l'Union européenne un régime homogène en matière d'accès à l'activité des banques et à l'exercice de cette activité.

[1] *Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.*

[2] *Capital Requirements Directive (CRD).*

Adoptée dans le cadre d'un paquet législatif élaboré en réaction à la crise économique et financière de 2008, la directive CRD renforce le cadre de surveillance prudentielle applicable au secteur bancaire. À ce titre, la directive CRD fixe les principales règles applicables en matière de surveillance prudentielle des établissements de crédit par les autorités nationales compétentes et de pouvoirs et outils de surveillance dont ces autorités disposent.

En particulier, le 1 de l'article 74 de la directive CRD prévoit l'obligation pour les établissements de crédit de disposer « d'un dispositif solide de gouvernance d'entreprise » qui doit comprendre notamment une structure organisationnelle claire, des processus efficaces de gestion des risques et des mécanismes adéquats de contrôle interne.

B. LE CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT, NOTAMMENT EN MATIÈRE DE GOUVERNANCE, A ÉTÉ TRANSPOSÉ EN DROIT NATIONAL DANS LE CODE MONÉTAIRE ET FINANCIER

Le cadre européen de surveillance prudentielle applicable au secteur bancaire a notamment été transposé en droit national par l'ordonnance du 20 février 2014 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière[1].

En particulier, en matière de gouvernance des établissements de crédit, l'article L. 511-55 du code monétaire et financier prévoit que ces établissements ont l'obligation de disposer d'un dispositif de gouvernance solide comprenant notamment une organisation claire, des procédures efficaces de gestion des risques et d'un dispositif adéquat de contrôle interne.

[1] *Ordonnance n° 2014-158 du 20 février 2014 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière.*

C. LA DIRECTIVE « DORA » DU 14 DÉCEMBRE 2022 A MIS À JOUR LE CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT EN MATIÈRE D'OBLIGATIONS RELATIVES À LA GOUVERNANCE POUR TENIR COMPTE DES RISQUES SPÉCIFIQUES LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

La directive (UE) 2022/2556 du 14 décembre 2022[1], ou « directive DORA »[2], prévoit plusieurs dispositions de mise à jour de la directive sectorielle CRD.

À ce titre, l'article 4 de la directive DORA prévoit d'actualiser le cadre de surveillance prudentielle fixé par la directive CRD.

En particulier, le 1 de l'article 74 de la directive CRD, qui fixe les obligations des établissements de crédit en matière de gouvernance, a été modifié pour inclure dans les obligations à la charge des établissements concernés celle d'inclure dans le dispositif de gouvernance des établissements « des réseaux et des systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554 ».

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI TRANSPOSE DANS LE DROIT NATIONAL LA MISE À JOUR, EN MATIÈRE DE GOUVERNANCE, DU CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT ET ÉTEND SON APPLICATION AUX SOCIÉTÉS DE FINANCEMENT

L'article 47 du projet de loi transpose la mise à jour du cadre prudentiel applicable aux établissements de crédit en matière de risque opérationnel et étend cette mise à jour aux sociétés de financement.

En premier lieu, l'article 47 prévoit la modification du premier alinéa de l'article L. 511-55 du code monétaire et financier pour prévoir que les établissements de crédit ont l'obligation de se doter d'un dispositif de gouvernance solide comprenant notamment des réseaux et des systèmes d'information mis en place et gérés conformément au règlement DORA[3].

En second lieu, en procédant à cette modification du cadre prudentiel applicable aux établissements de crédit, le projet de loi impose les mêmes

---

[1] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Digital Operational Resilience Act.*

[3] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

obligations actualisées en matière de gouvernance aux sociétés de financement qui sont assujetties aux obligations fixées par l'article L. 511-55 du code monétaire et financier.

III. LA POSITION DE LA COMMISSION SPÉCIALE : L'APPLICATION DU CADRE ACTUALISÉ DE SURVEILLANCE PRUDENTIELLE EN MATIÈRE DE GOUVERNANCE AUX ÉTABLISSEMENTS DE CRÉDIT ET AUX SOCIÉTÉS DE FINANCEMENT RÉPOND À LA NÉCESSITÉ DE TRANSPOSER LE DROIT DE L'UNION ET DE MAINTENIR UN TRAITEMENT HOMOGÈNE ENTRE LES ÉTABLISSEMENTS DE CRÉDIT ET LES SOCIÉTÉS DE FINANCEMENT

C. L'ACTUALISATION DU CADRE PRUDENTIEL APPLICABLE EN MATIÈRE DE GOUVERNANCE AUX ÉTABLISSEMENTS DE CRÉDIT RÉSULTE DE L'OBLIGATION CONSTITUTIONNELLE DE TRANSPOSITION DU DROIT DE L'UNION

La mise à jour des obligations applicables aux établissements de crédit en matière de risque opérationnel correspond à la transposition de la directive DORA en droit national par la modification du code monétaire et financier. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

D. L'EXTENSION DE LA MISE À JOUR DU CADRE PRUDENTIELLE APPLICABLE EN MATIÈRE DE GOUVERNANCE AUX SOCIÉTÉS DE FINANCEMENT EST LÉGITIME AU REGARD DE L'OBJECTIF DE MAINTIEN D'UN TRAITEMENT PRUDENTIEL HOMOGÈNE ENTRE CES DEUX ACTIVITÉS ET DU PRINCIPE DE PROPORTIONNALITÉ APPLICABLE À CE DISPOSITIF DE GOUVERNANCE

Les sociétés de financement, qui sont des sociétés qui exercent une activité professionnelle de crédit sans collecter des dépôts, sont soumis en France à un cadre prudentiel équivalent au cadre applicable au secteur bancaire[2]. Si le droit de l'Union ne prévoit pas d'obligation d'inclure ces sociétés dans le champ d'application du cadre prudentiel applicable aux établissements de crédit défini par la directive CRD, les autorités françaises ont choisi depuis 2013 d'appliquer à ces sociétés, sauf pour certaines

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*
[2] *En 2024, le nombre de sociétés de financement agréées en France était de 144.*

obligations spécifiques notamment en matière de liquidité et de levier, les mêmes obligations prudentielles que celles applicables au secteur bancaire.

Ce choix est fondé sur la volonté de permettre aux établissements de crédits de bénéficier d'un régime favorable pour leurs expositions sur les sociétés de financement dans le cadre du calcul déterminant leur respect des exigences de fonds propres applicables aux établissements de crédit.

En effet, l'article 119 du « règlement CRR »[1] du 26 juin 2013[2] prévoit que, dans le cadre du calcul des ratios de fonds propres soumis aux exigences prudentielles applicables aux établissements de crédit, les expositions sur les établissements financiers qui, sans entrer dans le champ du règlement, sont soumis à l'agrément et à la surveillance des autorités compétentes et respectent « des exigences prudentielles comparables » à celles applicables au secteur bancaire sont traitées comme des expositions sur les établissements de crédit.

Par surcroît, l'obligation de disposer d'un dispositif de gouvernance solide consacrée par l'article L. 511-55 du code monétaire et financier est appliquée en tenant compte d'un principe de proportionnalité. En effet, le dernier alinéa de cet article dispose que le dispositif de gouvernance « est adapté à la nature, à l'échelle et à la complexité des risques inhérents » au modèle d'entreprise et à ses activités. Ce principe de proportionnalité limite le risque que des sociétés de financement soit soumises, au titre de cet article, à des obligations disproportionnées au regard de leur taille et des risques qu'elles représentent.

Par suite, l'extension de la mise à jour du cadre prudentiel en matière de gouvernance est justifiée par le fait que les obligations pesant sur les sociétés de financement seront proportionnées à leurs risques et qu'elle permet de maintenir des exigences prudentielles homogènes entre les établissements de crédit et les sociétés de financement, ce qui permet de garantir le maintien d'un régime favorable pour les expositions sur les sociétés de financement dans le cadre du respect des exigences fixées par le règlement CRR.

Décision de la commission : la commission spéciale a adopté cet article sans modification.

---

[1] *Capital Requirement Regulation.*

[2] *Règlement (UE) n ° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n ° 648/2012.*

Article 48

Obligations des prestataires de services de paiement en matière de gestion du risque lié aux technologies de l'information et de la communication

Le présent article prévoit que les prestataires de services de paiement qui constituent des entités financières au sens du règlement DORA doivent se conformer aux exigences en matière de gestion du risque lié aux technologies de l'information et de la communication (TIC) énumérées au chapitre II du règlement DORA.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : UNE OBLIGATION GÉNÉRALE POUR LES PRESTATAIRES DE SERVICES DE PAIEMENT DE METTRE EN PLACE UN CADRE POUR LA GESTION DES RISQUES INFORMATIQUES

L'article L. 521-9 du code monétaire et financier (CMF) prévoit **l'obligation pour les prestataires de services de paiement** de mettre en place des **mesures d'atténuation et des mécanismes de contrôle** appropriés en vue de gérer les **risques opérationnels et de sécurité** liés aux services de paiement qu'ils fournissent. Cette obligation a été insérée dans le code monétaire et financier à l'occasion de la transposition de l'article 95 de la **directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015** concernant les services de paiement dans le marché intérieur (dite « **DSP2** »)[1].

Les dispositions de l'article L. 521-9 du CMF sont précisées par le titre VI bis de **l'arrêté du 3 novembre 2014 sur le contrôle interne**[2]. Les prestataires de service de paiement doivent établir et maintenir des **procédures efficaces de gestion des incidents**, y compris pour la **détection et la classification des incidents opérationnels et de sécurité majeurs**.

Ces procédures de gestion des incidents, intégrées aux procédures globales de gestion des risques des prestataires de services de paiement, doivent permettre à l'établissement concerné **d'identifier, de mesurer, de suivre et de gérer l'ensemble des risques** résultant des activités liées au paiement du prestataire de services de paiement et auxquels est exposé ce

[1] *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE. L'article 3 de la DSP2 a été transposée dans le droit national par l'article 17 de l'ordonnance n°2017-1433 du 4 octobre 2017.*

[2] *Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.*

prestataire, notamment en matière de continuité des activités. Elles comprennent notamment le **document relatif à la politique de sécurité**, et doivent définir et attribuer **les principaux rôles et responsabilités**, ainsi que le **système de déclaration** pertinents nécessaires pour faire appliquer les mesures de sécurité et pour gérer les risques opérationnels et de sécurité.

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI PRÉVOIT QUE LES PRESTATAIRES DE SERVICES DE PAIEMENT SE CONFORMENT AUX EXIGENCES DU CHAPITRE II DU RÈGLEMENT DORA SUR LA GESTION DU RISQUE LIÉ AUX TIC

Le présent article prévoit de **modifier l'article L. 521-9 du code monétaire et financier** afin de transposer **l'article 7 (4) de la directive DORA**.

L'article 7 (4) de la directive DORA prévoit de **compléter l'article 95 de la DSP2**, qui fixe **une obligation générale** de mise en place d'un cadre pour la gestion des risques informatiques. Il vise à préciser qu'outre ces dispositions générales, les prestataires de services de paiement doivent se conformer aux exigences - plus précises – contenues dans le **chapitre II du règlement DORA**[1], consacré à la **gestion du risque lié aux TIC**.

Comme déjà rappelé, le **chapitre II du règlement DORA** prévoit un **cadre harmonisé de gestion du risque lié aux TIC** que les entités financières doivent intégrer pour parer au risque lié aux TIC de manière rapide, efficiente et exhaustive, et garantir un niveau élevé de résilience opérationnelle numérique.

Ces mesures à mettre en place par les entités concernées comprennent notamment :

- la mise en place **d'un cadre de gouvernance et de contrôle interne**, ainsi qu'une stratégie de résilience opérationnelle numérique. Ce cadre de gestion des risques doit par exemple comprendre des systèmes, protocoles et outils de TIC qui doivent être tenus à jour ;
- **l'identification de toutes les sources de risques liés aux TIC** et l'évaluation de ces risques selon une classification devant être revue à minima une fois par an ;
- l'élaboration d'une politique de sécurité de l'information qui définit des règles visant ;
- **l'instauration d'une politique complète de continuité des activités de TIC**, ainsi que des procédures de sauvegarde, de restauration et de

[1] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

rétablissement. Cette politique comprend par exemple des tests à effectuer au moins une fois par an.

L'article **L. 521-9 du code monétaire et financier** est ainsi complété **pour préciser que les prestataires de services de paiement** se conforment également aux exigences du **chapitre II du règlement DORA**, qui porte sur la gestion du risque lié aux TIC.

III. LA POSITION DE LA COMMISSION : UN AJOUT NÉCESSAIRE POUR TENIR COMPTE EN DROIT INTERNE DE L'ADOPTION DU RÈGLEMENT DORA

Le présent article permet de **tirer les conséquences en droit interne** de l'adoption des dispositions du **chapitre II du règlement DORA**, qui sont **d'application directe**. Il permet de compléter l'article L. 521-9 du code monétaire et financier pour préciser que les prestataires de services de paiement doivent de se conformer **aux exigences en matière de gestion des risques TIC prévues par le chapitre II du règlement DORA**.

Décision de la commission : la commission a adopté l'article sans modification.

Article 49 A

Extension de l'application du règlement DORA aux succursales d'entreprises d'investissement de pays tiers

Le présent article additionnel, introduit par un amendement COM-129 du rapporteur Michel Canévet, prévoit d'étendre l'application du règlement DORA aux succursales d'entreprises d'investissement de pays tiers.

La commission a adopté l'article 49 A.

I. LE DROIT EXISTANT : LE RÈGLEMENT DORA S'IMPOSE AUX ENTREPRISES D'INVESTISSEMENT DONT LE SIÈGE EST DANS L'UNION EUROPÉENNE MAIS PAS AUX SUCCURSALES D'ENTREPRISES DE PAYS TIERS

Suivant la définition donnée par **l'article L. 531-4 du code monétaire et financier**, les **entreprises d'investissement** sont des personnes morales autres que les établissements de crédit, qui ont pour profession habituelle et principale de fournir des services d'investissement.

Les **succursales des entreprises d'investissement de pays tiers** sont régies par **l'article L. 532-48 du code monétaire et financier**. Cet article précise notamment les **conditions à remplir** pour que **l'ACPR délivre l'agrément** d'une succursale d'entreprise d'investissement de pays tiers en France.

L'article L. 532-50 du code monétaire et financier précise que les **succursales agréées d'entreprises d'investissement de pays tiers** doivent respecter **plusieurs dispositions prudentielles**, notamment celles définies par le règlement du 27 novembre 2019 sur les exigences prudentielles applicables aux entreprises d'investissement[1] ou encore certaines obligations du règlement du 15 mai 2024 sur les marchés d'instruments financier[2].

L'article 2 du règlement DORA[3] inclue les **entreprises d'investissement** dans **le champ d'application des entités financières couvertes par le règlement**[4]. En revanche, le règlement ne donne pas

[1] *Règlement (UE) 2019/2033 du Parlement européen et du Conseil du 27 novembre 2019 concernant les exigences prudentielles applicables aux entreprises d'investissement et modifiant les règlements (UE) n° 1093/2010, (UE) n° 575/2013, (UE) n° 600/2014 et (UE) n° 806/2014.*

[2] *Règlement (UE) n° 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les s et modifiant le règlement (UE) n° 648/2012.*

[3] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

[4] *Point e) de l'article 2 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

d'indication concernant **l'application ou non de la règlementation DORA aux succursales d'entreprises d'investissement de pays tiers.**

II. LE DISPOSITIF PROPOSÉ : ÉTENDRE L'APPLICATION DE DORA AUX SUCCURSALES D'ENTREPRISES D'INVESTISSEMENT DE PAYS TIERS

En l'état actuel, les **succursales d'entreprises d'investissement de pays tiers** ne sont pas tenues d'appliquer les exigences du règlement DORA. Or, pour des raisons **d'égalité de traitement**, ces succursales **devraient être soumises aux mêmes standards** que tout **autre acteur financier délivrant des services d'investissement en France.**

Cet article additionnel, introduit par un amendement COM-129 du rapporteur Michel Canévet, permet d'assurer une **égalité de traitement entre toutes les entreprises d'investissement établies en France**, et de garantir ainsi un **renforcement de la résilience cyber et informatique** des entités financières présentes en France.

De plus cette **mesure est cohérente avec l'approche historique** portée à travers cet article L. 532-50 du code monétaire et financier, pour intégrer les dispositions prudentielles qui s'appliquaient aux entreprises d'investissement.

Décision de la commission : la commission a adopté l'article additionnel.

Article 49

Modifications de la liste des prestataires de services de paiement soumis à une obligation de notification des incidents opérationnels

Le présent article prévoit que seuls les prestataires de services de paiement qui ne sont pas des entités financières au sens de DORA doivent notifier les incidents opérationnels majeurs à l'ACPR et les incidents de sécurité majeurs à la Banque de France, dispositifs prévus par la 2ème directive sur les services de paiement (DSP2).

La commission a adopté un amendement COM-128 du rapporteur Michel Canévet pour fusionner les notifications d'incidents prévues par la DSP2 et celles prévues par le règlement DORA, dans un souci de simplification.

Par ailleurs, cet amendement fait de l'ACPR le point d'entrée unique pour la réception des notifications d'incidents. Il met ainsi fin à l'exigence de notification des incidents de sécurité majeurs auprès de la Banque de France. Cette dernière conserve toutefois la prérogative de prendre des mesures appropriées en réponse à un incident majeur, en en informant l'ACPR.

La commission a adopté l'article 49 ainsi modifié.

I. LE DROIT EXISTANT : UNE OBLIGATION DE NOTIFICATION DES INCIDENTS OPÉRATIONNELS ET DE SÉCURITÉ LIÉS AU PAIEMENT EXISTE DÉJÀ EN DROIT INTERNE, DU FAIT DE LA TRANSPOSITION DE LA DSP2

L'article L. 521-10 du code monétaire et financier (CMF) prévoit que les prestataires de services de paiement doivent informer **sans retard injustifié l'Autorité de contrôle prudentiel et de résolution (ACPR) de tout incident opérationnel majeur** et la **Banque de France en cas d'incident de sécurité majeur.**

Ces obligations de notification ont été inscrites dans le CMF à la suite de la transposition de l'article 96 de la **directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur** (dite « **DSP2** »)[1].

Lorsque l'incident a ou est susceptible d'avoir des répercussions sur les intérêts financiers de ses utilisateurs de services de paiement, le prestataire de services de paiement informe sans retard injustifié **ses utilisateurs de services de paiement de l'incident** et de toutes les mesures disponibles qu'ils peuvent prendre pour atténuer les effets dommageables de l'incident. Dès

[1] *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE. L'article 96 de la DSP2 a été transposé via l'article 12 de l'ordonnance n° 2017-1252 du 9 août 2017.*

réception de ces notifications, l'ACPR ou la Banque de France communique sans retard injustifié les détails importants de l'incident à **l'Autorité bancaire européenne et à la Banque centrale européenne**, et, après avoir évalué la pertinence de l'incident pour d'autres autorités nationales concernées, informe celles-ci en conséquence.

Pour rappel, l'article **L. 521-1 du CMF** distingue **deux catégories de prestataires de services de paiement**. La première regroupe les **établissements de paiement, les établissements de monnaie électronique, les établissements de crédit et les prestataires de services d'information sur les comptes**. La seconde rassemble **des institutions publiques** qui peuvent fournir des services de paiement : la Banque de France, l'Institut d'émission des départements d'outre-mer et l'Institut d'émission d'outre-mer, le Trésor public et la Caisse des dépôts et consignations[1]. **Ces deux catégories** de prestataires de services de paiement sont soumises aux **obligations de notification des incidents opérationnels prévues par la DSP2**.

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI PRÉVOIT DE RESTREINDRE LES OBLIGATIONS DE NOTIFICATION PRÉVUES PAR LA DSP2 AUX PRESTATAIRES DE SERVICES DE PAIEMENT QUI NE SONT PAS DES ENTITÉS FINANCIÈRES AU SENS DE DORA

Le présent article prévoit de **modifier l'article L. 521-10 du code monétaire et financier** afin de permettre la transposition de **l'article 7 (5) de la directive DORA.**

L'article 7 (5) de la directive DORA exclut du champ de l'obligation de notification des incidents au titre du DSP2 **les prestataires de services de paiement qui constituent des entités financières au sens du règlement DORA**[2]. Les notifications au titre de DORA sont réputées satisfaire les obligations de notifications au titre de la DSP2, ce qui évite ainsi un doublon en matière de déclaration.

Dès lors, le présent article prévoit de limiter **aux prestataires de services de paiement qui ne sont pas des entités financières au sens de DORA**, à savoir les **institutions publiques** listées au **II de l'article L521-1 du CMF**, les obligations de notification des incidents au titre de la DSP2. Les entités financières au sens de DORA quant à elles **n'ont pas à se conformer** à ces exigences puisqu'elles sont soumises à des **exigences équivalentes** avec la règlementation DORA.

---

[1] *II de l'article L521-1 du code monétaire et financier.*

[2] *Les entités financières au sens de DORA sont les établissements de crédit, les établissements de monnaie électronique et les établissements de paiement, respectivement mentionnés aux points a) b) et d) de l'article 1er de la DSP2.*

III. LA POSITION DE LA COMMISSION : UNE NÉCESSAIRE RÉÉCRITURE COMPLÈTE DE L'ARTICLE POUR CLARIFIER LES EXIGENCES DE NOTIFICATION ET DÉSIGNER L'ACPR COMME POINT D'ENTRÉE UNIQUE

A. UN BESOIN DE SIMPLIFICATION, QUI DOIT PASSER PAR UNE FUSION DES DÉCLARATIONS D'INCIDENTS PRÉVUES PAR LA DSP2 ET PAR DORA

Le présent article du projet de loi est source de complexité et de confusion. Il maintient de fait une distinction entre les **obligations de notification au titre de la DSP2 et celles au titre de DORA**. Or, **l'article 23 du règlement DORA** permet **de fusionner ces obligations de *reporting***[1] pour les entités qui sont soumises à ces doubles obligations, à savoir les entités financières au sens de Dora. Il est donc proposé une **récriture complète de l'article L. 521-10 du code monétaire et financier** afin d'y intégrer la **référence au règlement DORA du 14 décembre 2022** (ce qui n'est pas le cas dans le présent article) et de permettre la **fusion pour ces entités des exigences de notification DORA et celles prévues par la DSP2**.

En complément, l'amendement COM-128 du rapporteur Michel Canévet permet de préciser que les déclarations d'incidents se font conformément aux conditions prévues par **l'article 19 du règlement DORA, sauf pour les institutions publiques**, qui n'entrent pas dans le champ de DORA, et qui sont listées au **II de l'article L. 521-1 du CMF**. Comme rappelé, ces institutions comprennent la Banque de France, l'Institut d'émission des départements d'outre-mer et l'Institut d'émission d'outre-mer, le Trésor public et la Caisse des dépôts et consignations.

L'amendement du rapporteur exclut néanmoins la **Caisse des dépôts et consignations (CDC)** des **entités publiques qui ne sont pas soumises à DORA.** Autrement dit, à la différence des autres institutions du II de l'article L. 521-1 du CMF, la **Caisse des dépôts et consignations serait assujettie aux exigences de notification prévues dans DORA**. La direction générale du Trésor et l'ACPR ont indiqué au rapporteur qu'il était en effet prévu de soumettre la CDC à ces exigences de DORA, par une future modification du décret régissant son cadre prudentiel. Une refonte du décret n°2020-94 du 5 février 2020 relatif au contrôle interne et externe de la CDC est actuellement en cours (son adoption prévue au printemps) et devrait prévoir l'application de DORA à la CDC ainsi que les adaptations nécessaires.

---

[1] *Article 23 du règlement DORA : Les exigences énoncées au présent chapitre s'appliquent également aux incidents opérationnels ou de sécurité liés au paiement et aux incidents opérationnels ou de sécurité majeurs liés au paiement lorsqu'ils concernent des établissements de crédit, des établissements de paiement, des prestataires de services d'information sur les comptes et des établissements de monnaie électronique.*

B. LA NÉCESSITÉ D'UN POINT D'ENTRÉE UNIQUE POUR LA NOTIFICATION PAR LES ENTITÉS FINANCIÈRES DES INCIDENTS LIÉS AU PAIEMENT

Dans sa rédaction actuelle et dans la rédaction proposée par l'article 49 du projet de loi, **l'article L. 521-10 du code monétaire et financier maintient la distinction entre les incidents de sécurité majeurs** – qui doivent être notifiés à la Banque de France – et les **incidents opérationnels majeurs** – qui doivent être déclarés à l'ACPR.

L'amendement du rapporteur permet **de supprimer cette distinction**, afin d'établir **l'ACPR comme l'autorité unique recevant les notifications d'incident.** Cette disposition permet de **simplifier** la procédure de notification pour les prestataires de services de paiement, qui n'ont plus à s'interroger sur l'autorité compétente à laquelle transmettre la déclaration d'incident. L'établissement **d'un point d'entrée unique** est une des demandes exprimées par les prestataires de services de paiement dans le cadre de l'application de la règlementation DORA.

L'amendement du rapporteur précise cependant que l'ACPR **communique ces incidents** et, le cas échéant, **les mesures prises**, à la **Banque de France** aux fins de l'accomplissement par celle-ci de ses missions. La Banque de France reste en effet **compétente pour prendre les mesures appropriées s'agissant de la sécurité des systèmes de paiement**[1].

Décision de la commission : la commission a adopté cet article ainsi modifié.

[1] *Le I de l''article L. 141-4 du code monétaire et financier précise ainsi que « La Banque de France veille au bon fonctionnement et à la sécurité des systèmes de paiement dans le cadre de la mission du Système européen de banques centrales relative à la promotion du bon fonctionnement des systèmes de paiement prévue par l'article 105, paragraphe 2 du traité instituant la Communauté européenne ».*

Article 50

Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement

Le présent article vise à transposer dans le droit interne le deuxième paragraphe de l'article 4 de la directive « DORA ».

Ce faisant, il prévoit que les dispositifs de contrôle et de sauvegarde des systèmes informatiques, dont disposent les établissements de crédits et les entreprises d'investissement fournissant des services d'investissement, incluent les réseaux et systèmes d'information mis en place et gérés conformément au règlement « DORA ».

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : LE DROIT INTERNE PRÉVOIT DÉJÀ QUE LES PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUTRES QUE LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE DISPOSENT DE DISPOSITIFS EFFICACES DE CONTRÔLE ET DE SAUVEGARDE DE LEURS SYSTÈMES INFORMATIQUES, SANS POUR AUTANT SE RÉFÉRER AUX EXIGENCES FIXÉES PAR LE PAQUET « DORA »

Aux termes de l'article L. 531-1 du code monétaire et financier, les prestataires de services d'investissement sont des établissements de crédit, des entreprises d'investissement ou des sociétés de gestion de portefeuille ayant reçu un agrément pour fournir des services d'investissement, listés à l'article L. 321-1 du code monétaire et financier[1].

L'article L. 533-2 du même code prévoit que les prestataires de services d'investissement (PSI) autres que les sociétés de gestion de portefeuille (SGP) disposent notamment de **dispositifs efficaces de contrôle et de sauvegarde de leurs systèmes informatiques**, sans qu'il ne soit fait référence à une quelconque réglementation européenne en la matière.

Or l'article 4 de la directive (UE) 2022/2556 du 14 décembre 2022[2], dite « DORA », en son deuxième paragraphe, modifie l'article 74 de la

[1] *Il s'agit de la réception, la transmission et l'exécution d'ordres pour le compte de tiers, la négociation pour compte propre, la gestion de portefeuille pour le compte de tiers, le conseil en investissement, la prise ferme, le placement garanti, le placement non garanti, et l'exploitation d'un système multilatéral ou organisé de négociation.*

[2] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

directive « CRD »[1] relatif à la gouvernance interne des établissements de crédit et des entreprises d'investissement, de façon à prévoir que les réseaux et systèmes d'information soutenant leur dispositif de gouvernance sont mis en place et gérés conformément au règlement (UE) 2022/2554 du 14 décembre 2022, dit règlement « DORA » [2].

II. LE DISPOSITIF PROPOSÉ : LES RÉSEAUX ET SYSTÈMES D'INFORMATION SOUTENANT LA GOUVERNANCE DES PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUTRES QUE LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE DOIVENT ÊTRE MIS EN PLACE ET GÉRÉS CONFORMÉMENT AUX RÈGLEMENT « DORA »

Le présent article modifie l'article L. 533-2 du code monétaire et financier afin de prévoir, comme l'article 47 le prévoit pour les établissements de crédit, que les dispositifs de contrôle et de sauvegarde des systèmes informatiques dont disposent les PSI autre que les SGP incluent les réseaux et systèmes d'information mis en place et gérés conformément au règlement « DORA ». Il s'agit donc d'une transposition, dans le droit interne, de la directive « CRD » dans sa rédaction issue de la directive « DORA ».

III. LA POSITION DE LA COMMISSION : UNE ÉVOLUTION NÉCESSAIRE POUR APPLIQUER LES CRITÈRES PRÉVUS PAR LE RÈGLEMENT « DORA » À LA GESTION DU RISQUE CYBER DES PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUTRES QUE LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE

Le présent article constitue une transposition indispensable du droit européen pour la mise en place d'un cadre de gestion du risque cyber par les établissements de crédit et les entreprises d'investissement, dont la résilience face aux cyberattaques et, plus généralement, au risque « TIC » doit être assurée, leur rôle dans le fonctionnement d'une économie de marché étant incontournable. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[3].

Décision de la commission : la commission a adopté cet article sans modification

---

[1] *Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.*

[2] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

[3] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 51

Systèmes de technologies de l'information et de la communication (TIC) et dispositifs de contrôle des prestataires de services d'investissement

Le présent article vise à transposer dans le droit interne l'article 1er et le premier paragraphe de l'article 6 de la directive « DORA ».

Ce faisant, il prévoit que les sociétés de gestion de portefeuille (SGP), à l'exception de celles qui gèrent certaines catégories de fonds d'investissements alternatifs, mettent en place des procédures administratives et comptables saines, des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris les réseaux et systèmes d'information mis en place et gérés conformément au règlement « DORA ».

Il prévoit par ailleurs que les systèmes mis en place par les prestataires de services d'investissement (PSI) autres que les SGP pour garantir la continuité, la régularité et le caractère satisfaisant de la fourniture des services d'investissement sont appropriés et proportionnés et incluent des systèmes de technologies de l'information et de la communication mis en place et gérés conformément à l'article 7 du règlement « DORA ».

Il prévoit enfin que les mécanismes de sécurité dont doivent disposer les PSI autres que les SGP assurent la sécurité et l'authentification des moyens de transfert de l'information se conforment aux exigences fixées par le règlement « DORA ».

La commission a adopté cet article sans modification.

I. LE DROIT INTERNE IMPOSE AUX PRESTATAIRES DE SERVICES D'INVESTISSEMENT DES MESURES DESTINÉES À GARANTIR LA CONTINUITÉ ET LA RÉGULARITÉ DE LA FOURNITURE DE CES SERVICES MAIS N'INTÈGRE PAS LES COMPLÉMENTS APPORTÉS PAR LA DIRECTIVE « DORA »

A. SI LES OBLIGATIONS PESANT SUR LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE SONT PLUS LÉGÈRES, L'ENSEMBLE DES PRESTATAIRES DE SERVICES D'INVESTISSEMENT DOIVENT DÉJÀ METTRE EN ŒUVRE DES MESURES DESTINÉES À GARANTIR LA CONTINUITÉ ET LA RÉGULARITÉ DE LA FOURNITURE DES SERVICES D'INVESTISSEMENTS

L'article L. 533-10 du code monétaire et financier détermine les **règles d'organisation applicables aux prestataires de services d'investissement**

(PSI)[1], et prévoit notamment la mise en place de mesures destinées à empêcher les conflits d'intérêt et à **garantir la continuité et la régularité de la fourniture des services d'investissement**, notamment lorsqu'elles confient à des tiers des fonctions opérationnelles importantes. Son I vise les **sociétés de gestion de portefeuille** (SGP) tandis que son II vise les PSI autres que les SGP.

Pour mémoire, les **sociétés de gestion de portefeuille** sont les personnes morales qui gèrent un ou plusieurs **organismes de placement collectif en valeurs mobilières** (OPCVM)[2] ou bien **des fonds d'investissement alternatif** (FIA)[3], de droit européen ou de droit étranger, ou d'autres placements collectifs[4]. Les fonds d'investissements alternatifs (en anglais, « *hedge funds* ») sont encadrés par les articles L. 214-24 à L. 214-190-3-1 du code monétaire et financier : distincts des OPCVM, ils lèvent des capitaux auprès d'un certain nombre d'investisseurs en vue de les investir, dans l'intérêt de ces investisseurs, conformément à une politique d'investissement que ces FIA ou leurs sociétés de gestion définissent[5]. Très divers, ils regroupent des fonds ouverts à des investisseurs non professionnels (comme les fonds de capital investissement, les organismes de placement collectif immobilier, les sociétés civiles de placement immobilier ou les sociétés d'épargne forestière), des fonds ouverts à des investisseurs professionnels, des fonds d'épargne salariale, et des organismes de financement (organismes de titrisation, mentionnés au I de l'article L. 214-167, et organismes de financement spécialisé).

S'agissant spécifiquement des **SGP**, **les seules obligations, très générales**, qui s'imposent à elles en matière de gestion du risque consistent à prendre des mesures raisonnables pour **garantir la continuité et la régularité de la fourniture des services d'investissement**, notamment lorsqu'elles confient à des tiers des fonctions opérationnelles importantes[6].

Ces obligations s'imposent également aux PSI autres que les SGP, mais s'y ajoute la garantie du « *caractère satisfaisant* » de la fourniture de ces services. La formule usitée pour le recours aux tiers est légèrement plus large : il s'agit des cas où ils leurs confient « *des fonctions ou d'autres tâches opérationnelles essentielles ou importantes* ». Il est précisé que « *dans ce cas, ils prennent des mesures raisonnables pour éviter une aggravation indue du risque opérationnel* »[7]. **Les PSI autres que les SGP doivent également disposer de**

---

[1] *Pour une définition, se reporter à l'article L. 531-1 du code monétaire et financier ou bien au commentaire de l'article précédent.*

[2] *Il s'agit d'un portefeuille dont les fonds investis sont placés en valeurs mobilières ou autres instruments financiers. Les OPCVM regroupent les Sicav (sociétés d'investissement à capital variable) et les FCP (fonds communs de placement).*

[3] *Régis par la directive 2011/61/UE du Parlement européen et du Conseil du 8 juin 2011 dite « AIFM », ils répondent à des contraintes réglementaires plus souples que les OPCVM.*

[4] *Article L. 532-9 du code monétaire et financier.*

[5] *Article L. 214-24 du code monétaire et financier.*

[6] *4° du I de l'article L. 533-10 du code monétaire et financier.*

[7] *4° du II de l'article L. 533-10 du code monétaire et financier.*

mécanismes de sécurité solides pour garantir la sécurité et l'authentification des moyens de transfert de l'information, réduire au minimum le risque d'altération de données et d'accès non autorisé et empêcher les fuites d'information afin de maintenir en permanence la confidentialité des données[1].

B. LA DIRECTIVE « DORA » COMPLÈTE LES OBLIGATIONS DE CONTRÔLE DE L'ENSEMBLE DES PRESTATAIRES D'INVESTISSEMENT POUR GARANTIR LA CONTINUITÉ ET LA RÉGULARITÉ DE LEURS ACTIVITÉS

Or, d'une part, en son paragraphe premier, **l'article 1er de la directive** (UE) 2022/2556 du 14 décembre 2022[2], dite **« DORA », en modifiant l'article 12 de la directive « OPCVM »[3], prévoit des dispositions plus précises,** que doivent respecter les sociétés de gestion dont l'activité habituelle est la gestion d'organismes de placement collectif de valeurs mobilières (OPCVM) et excluant donc celles qui gèrent des fonds d'investissement alternatifs (FIA). Elles doivent notamment avoir des **procédures administratives et comptables saines ainsi que des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris en ce qui concerne les réseaux et les systèmes d'information qui sont mis en place et gérés conformément au règlement « DORA ».** Ces dispositions ne sont actuellement pas transposées dans le droit français s'agissant des sociétés de gestion de portefeuille concernées.

D'autre part, au a) de son premier paragraphe, **l'article 6 de la directive « DORA », en modifiant l'article 16 de la directive « MIF 2 »[4], prévoit que les systèmes que doivent utiliser les entreprises d'investissement** – c'est-à-dire les PSI autres que les SGP – pour garantir la continuité et la régularité de la fourniture de ses services d'investissement et de l'exercice de ses activités d'investissement **incluent les systèmes de technologies de l'information et de la communication mis en place et gérés conformément à l'article 7 du** règlement (UE) 2022/2554 du 14 décembre 2022, ou « règlement DORA »[5], dit **« DORA ».** Ce dernier impose aux entités

---

[1] *5° du II de l'article L. 533-10 du code monétaire et financier.*

[2] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[3] *Directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM).*

[4] *Directive 2014/65/UE du Parlement européen et du Conseil u 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.*

[5] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

financières d'utiliser et de tenir à jour des **systèmes, protocoles et outils de TIC adaptés, fiables, dotés d'une capacité de traitement suffisante et suffisamment résilients sur le plan technologique**. Ces dispositions ne sont actuellement pas transposées dans le droit français s'agissant des PSI autres que les SGP.

Au b) du même paragraphe, l'article 6 de la directive « DORA » prévoit que les mécanismes de sécurité dont doivent disposer les entreprises d'investissement assurent la sécurité et l'authentification des moyens de transfert de l'information se conforment aux exigences fixées par le règlement « DORA ».

II. LE DISPOSITIF PROPOSÉ : RENFORCER CONFORMÉMENT AU PAQUET « DORA » LES OBLIGATIONS DES PRESTATAIRES DE SERVICES D'INVESTISSEMENT RELATIVES AU TRAITEMENT ÉLECTRONIQUE DES DONNÉES, À LA CONTINUITÉ DES ACTIVITÉS, À LA SÉCURITÉ ET À L'AUTHENTIFICATION DES TRANSFERTS D'INFORMATIONS

Le présent article vise à **transposer dans le droit français les dispositions de la directive « DORA » relatives à l'organisation interne des PSI pour traiter le risque cyber.**

Transposant le paragraphe 1er de l'article 1er de la directive, le 1° modifie le I de l'article L. 533-10 du code monétaire et financier (CMF) pour prévoir que **les SGP**, à l'exception de celles qui gèrent certaines catégories de fonds d'investissements alternatifs (FIA dont le volume d'actifs est limité et qui doivent obtenir l'agrément de l'Autorité des marchés financiers, relevant du IV de l'article L. 532-9 du CMF, et organismes de titrisation relevant du I de l'article L. 214-167 du CMF), **mettent en place des procédures administratives et comptables saines, des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris les réseaux et systèmes d'information mis en place et gérés conformément au règlement « DORA ».**

Transposant le a) du paragraphe 1er de l'article 6 de la directive, le a) du 2° du présent article modifie le II de l'article L. 533-10 du CMF pour prévoir que les **systèmes mis en place par les PSI autres que SGP pour garantir la continuité, la régularité et le caractère satisfaisant de la fourniture des services d'investissement sont appropriés et proportionnés et incluent des systèmes de technologies de l'information et de la communication mis en place et gérés conformément à l'article 7 du règlement « DORA ».**

Transposant le b) du même paragraphe du même article, le b) du 2° en reprend les termes et prévoit que **les mécanismes de sécurité dont doivent disposer les PSI autres que SGP assurent la sécurité et l'authentification des**

moyens de transfert de l'information se conforment aux exigences fixées par le règlement « DORA ».

III. LA POSITION DE LA COMMISSION : UNE ÉVOLUTION NÉCESSAIRE POUR RACCROCHER LE TRAITEMENT DU RISQUE CYBER PAR LES PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUX CRITÈRES PRÉVUS PAR LE RÈGLEMENT « DORA »

Le présent article constitue une **transposition nécessaire du droit européen en matière de traitement technique du risque cyber par les prestataires de service d'investissement**, dont la résilience face aux cyberattaques et, plus généralement, au risque « TIC » doit être assurée. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

Décision de la commission : la commission a adopté cet article sans modification

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 52

Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique

Le présent article vise à transposer dans le droit interne le deuxième paragraphe de l'article 6 de la directive « DORA ».

Ce faisant, il impose la conformité aux exigences fixées au chapitre II du règlement « DORA » des systèmes et contrôles des risques destinés à garantir la résilience et la capacité des systèmes de négociation algorithmique gérés par des prestataires de services d'investissement autres que les sociétés de gestion de portefeuille.

Par ailleurs, il prévoit que les mécanismes de continuité des activités destinés à faire face à toute défaillance de ces systèmes de négociation incluent une politique et des plans de continuité des activités ainsi que de plans de réponses et de rétablissement, conformément à l'article 11 du règlement « DORA ». Les systèmes doivent être testés et suivis pour garantir qu'ils satisfont aux exigences spécifiques fixées aux chapitres II et IV de ce règlement.

La commission a adopté cet article sans modification.

I. LES OBLIGATIONS DES PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUTRES QUE LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE QUI ONT RECOURS À LA NÉGOCIATION ALGORITHMIQUE EN MATIÈRE DE SUIVI DU RISQUE CYBER ET DE CONTINUITÉ DES ACTIVITÉS NE SONT PAS CONFORMES À LA DIRECTIVE « DORA »

Le *trading* algorithmique consiste à utiliser des plateformes qui automatisent la saisie des ordres de bourse en laissant un algorithme décider des différents paramètres de l'ordre (prix de saisie, volume des positions, instants d'ouverture et de clôture) en autonomie.

L'article L. 533-10-4 du code monétaire et financier (CMF) prévoit que les prestataires de services d'investissement (PSI) autres que les sociétés de gestion de portefeuille (SGP)[1], qui ont recours à la **négociation algorithmique,** disposent de **système et contrôles des risques destinés à garantir, notamment, que leurs systèmes de négociation sont résilients et ont une capacité suffisante** (a du 1° de l'article). Il est également prévu qu'ils disposent de **plans de continuité des activités efficaces pour faire face à toute**

[1] *Pour une définition, voir les commentaires d'articles précédents ou l'article L. 531-1 du code monétaire et financier.*

défaillance de leurs systèmes de négociation et veillent à ce que ces derniers soient entièrement testés et convenablement suivis de manière à garantir leur conformité aux exigences du présent article (2° de l'article).

Ces dispositions constituent une transposition du premier paragraphe de l'article 17 de la directive « MIF 2 »[1] dans sa rédaction en date du 15 mai 2014. Celui-ci a été modifié par le paragraphe 2 de l'article 6 de la directive (UE) 2022/2556 du 14 décembre 2022[2], dite « DORA », prévoit la conformité aux exigences fixées au chapitre II du règlement (UE) 2022/2554 du 14 décembre 2022[3], dit règlement « DORA »[4], des systèmes et contrôles des risques destinés à garantir la résilience et la capacité des systèmes de négociation. Il prévoit également que les mécanismes de continuité des activités destinés à faire face à toute défaillance des systèmes de négociation inclut une politique et des plans en matière de continuité des activités de TIC et de plans de réponses et de rétablissement des TIC mis en place conformément à l'article 11 du règlement « DORA »[5]. Il dispose enfin que les systèmes sont testés et suivis pour garantir qu'ils satisfont aux exigences spécifiques fixées aux chapitres II et IV du règlement « DORA »[6].

II. LE DISPOSITIF PROPOSÉ : UNE MISE EN CONFORMITÉ AVEC LA PAQUET « DORA » DES OBLIGATIONS EN MATIÈRE DE GESTION DU RISQUE CYBER QUI S'IMPOSENT AUX PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUTRES QUE LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE QUI ONT RECOURS À LA NÉGOCIATION ALGORITHMIQUE

Le présent article vise à transposer dans le droit interne le deuxième paragraphe de l'article 6 de la directive « DORA ».

En son **1°**, il modifie ainsi le a) du 1° de l'article L. 533-10-4 du CMF de façon à prévoir la conformité aux exigences fixées au chapitre II du règlement « DORA »[7] des systèmes et contrôles des risques destinés à garantir la résilience et la capacité des systèmes de négociation algorithmiques gérés par des PSI autres que des SGP.

---

[1] *Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.*

[2] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[3] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

[4] *Voir les commentaires des articles précédents pour plus de précisions.*

[5] *Idem.*

[6] *Idem.*

[7] *Voir les commentaires d'articles précédents pour des précisions sur le contenu de ce chapitre.*

En son **2°**, il modifie ensuite le 2° du même article de façon à prévoir que les mécanismes de continuité des activités destinés à faire face à toute défaillance des systèmes de négociation incluent une politique et des plans en matière de continuité des activités de TIC et de plans de réponses et de rétablissement des TIC mis en place conformément à l'article 11 du règlement « DORA », et que les systèmes sont testés et suivis pour garantir qu'ils satisfont aux exigences spécifiques fixées aux chapitres II et IV de ce règlement.

III. LA POSITION DE LA COMMISSION : UNE ÉVOLUTION NÉCESSAIRE POUR APPLIQUER LES CRITÈRES PRÉVUS PAR LE RÈGLEMENT « DORA » À LA GESTION DU RISQUE CYBER PAR LES PRESTATAIRES DE SERVICES D'INVESTISSEMENT AUTRES QUE LES SOCIÉTÉS DE GESTION DE PORTEFEUILLE QUI ONT RECOURS À LA NÉGOCIATION ALGORITHMIQUE

Le présent article constitue une transposition nécessaire du droit européen en matière de gestion du risque cyber par les PSI autres que les SGP ayant recours à la négociation algorithmique, lesquels peuvent être particulièrement sensibles aux cyberattaques. Leur résilience face au risque « TIC » doit être assurée. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

Décision de la commission : la commission a adopté cet article sans modification

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 53

Références aux prestataires informatiques critiques au sein des tiers auxquels l'Autorité de contrôle prudentiel et de résolution peut demander toute information

Le présent article prévoit de mentionner expressément les prestataires tiers de services fondés sur les technologies de l'information et de la communication (TIC) parmi les personnes entrant dans le périmètre du droit de communication dont dispose le secrétaire général de l'Autorité de contrôle prudentiel et de résolution (SGACPR) dans le cadre de l'accomplissement de ses missions.

La rédaction actuelle du code monétaire et financier prévoit déjà que les tiers auprès desquels les établissements de crédit et les sociétés de financement ont externalisé des fonctions ou activités opérationnelles entrent dans le champ du droit de communication du SGACPR.

Par conséquent, cet article complexifie la rédaction de l'article L. 612-24 du code monétaire et financier sans apporter de modification substantielle au droit applicable.

La commission spéciale a supprimé cet article.

I. LE DROIT EXISTANT : L'AUTORITÉ DE CONTRÔLE PRUDENTIELLE ET DE RÉSOLUTION DISPOSE D'UN LARGE DROIT DE COMMUNICATION DES INFORMATIONS UTILES À L'ACCOMPLISSEMENT DE SES MISSIONS

A. LA DIRECTIVE SECTORIELLE « CRD » DU 26 JUIN 2013 PRÉVOIT QUE LES AUTORITÉS DE SURVEILLANCE PRUDENTIELLE DISPOSENT DE POUVOIRS ÉLARGIS DE CONTRÔLE POUR EXERCER LEURS MISSIONS

La directive 2013/36/UE du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement[1], ou directive « CRD »[2], est une directive sectorielle ayant pour objet de fixer au sein de l'Union européenne un régime homogène en matière d'accès à l'activité des banques et à l'exercice de cette activité.

[1] *Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.*

[2] *Capital Requirements Directive (CRD).*

Adoptée dans le cadre d'un paquet législatif élaboré en réaction à la crise économique et financière de 2008, la directive CRD renforce le cadre de surveillance prudentielle applicable au secteur bancaire. À ce titre, la directive CRD fixe les principales règles applicables en matière de surveillance prudentielle des établissements de crédit par les autorités nationales compétentes et de pouvoirs et outils de surveillance dont ces autorités disposent.

En particulier, le 3 de l'article 65 de la directive CRD prévoit que les autorités compétentes sont investies d'un pouvoir de collecte d'informations en application duquel elles peuvent exiger la fourniture de toute information nécessaire à l'accomplissement de leurs missions à plusieurs catégories de personnes physiques et morales dont notamment les tiers auprès desquels les établissements assujettis au contrôle prudentiel ont externalisé des fonctions ou des activités opérationnelles.

B. LE CADRE DE SURVEILLANCE PRUDENTIELLE APPLICABLE À L'ACTIVITÉ DES ÉTABLISSEMENTS DE CRÉDIT, NOTAMMENT EN MATIÈRE DE DROIT DE COMMUNICATION DE L'AUTORITÉ DE CONTRÔLE PRUDENTIEL ET DE RÉSOLUTION, A ÉTÉ TRANSPOSÉ EN DROIT NATIONAL DANS LE CODE MONÉTAIRE ET FINANCIER

Le cadre européen de surveillance prudentielle applicable au secteur bancaire a notamment été transposé en droit national par l'ordonnance du 20 février 2014 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière[1].

L'autorité nationale chargée, conjointement avec la Banque centrale européenne, de la surveillance prudentielle du secteur bancaire est l'Autorité de contrôle prudentiel et de résolution (ACPR) qui contrôle le respect par les personnes assujetties au contrôle prudentiel des dispositions européennes qui leur sont directement applicable ainsi que des dispositions du code monétaire et financier[2].

Dans ce cadre, en matière de pouvoir de collecte d'information de l'Autorité de contrôle prudentiel et de résolution (ACPR), le troisième alinéa de l'article L. 612-24 du code monétaire et financier consacre un droit de communication élargi du secrétaire général de l'Autorité de contrôle prudentiel et de résolution (SGACPR) qui peut, dans le cadre de l'accomplissement de ses missions, demander « tous renseignements, documents, quel qu'en soit le support, et en obtenir la copie » a plusieurs

---

[1] *Ordonnance n° 2014-158 du 20 février 2014 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière.*
[2] *Article L. 612-1 du code monétaire et financier.*

catégories de personnes dont les tiers auprès desquels des assujettis ont externalisé des fonctions ou activités opérationnelles.

C. LA DIRECTIVE « DORA » DU 14 DÉCEMBRE 2022 A MIS À JOUR LE CADRE DE SURVEILLANCE PRUDENTIELLE EN MATIÈRE DE POUVOIR DE COLLECTE D'INFORMATIONS DES AUTORITÉS DE SURVEILLANCE POUR TENIR COMPTE DES RISQUES SPÉCIFIQUES LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

La directive (UE) 2022/2556 du 14 décembre 2022[1], ou « directive DORA »[2], prévoit plusieurs dispositions de mise à jour de la directive sectorielle CRD.

À ce titre, l'article 4 de la directive DORA prévoit d'actualiser le cadre de surveillance prudentielle fixé par la directive CRD.

En particulier, le 3 de l'article 65 de la directive CRD, qui fixe la liste des catégories de personnes auprès desquelles les autorités compétentes peuvent exercer leur pouvoir de collecte d'information, est modifié pour mentionner expressément « les prestataires tiers de services TIC » visés au chapitre V du règlement DORA[3].

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI PRÉVOIT D'INSCRIRE EXPRESSÉMENT DANS LE DROIT NATIONAL L'INCLUSION DES PRESTATAIRES TIERS DE SERVICES FONDÉS SUR LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC) DANS LE CHAMP DU POUVOIR DE COLLECTE D'INFORMATIONS DE L'ACPR

L'article 53 du projet de loi transpose la mise à jour du cadre prudentiel en matière de pouvoir de collecte d'informations du secrétaire général de l'Autorité de contrôle prudentiel et de résolution.

À ce titre, l'article 53 prévoit d'insérer au troisième alinéa de l'article L. 612-24 du code monétaire et financier, qui dispose que le SGACPR dispose d'un pouvoir de collecte d'informations auprès des tiers auxquels les assujettis ont externalisé des fonctions ou activités opérationnelles, la mention expresse que ce pouvoir s'applique « y compris [sur] les prestataires tiers, en particulier

---

[1] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Digital Operational Resilience Act.*

[3] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

critiques, des services fondés sur les technologies de l'information et de la communication » visés au chapitre V du règlement DORA[1].

III. LA POSITION DE LA COMMISSION SPÉCIALE : LA RÉDACTION ACTUELLE DU CODE MONÉTAIRE ET FINANCIER PERMET DÉJÀ D'INCLURE LES PRESTATAIRES TIERS DE SERVICES FONDÉS SUR LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC) DANS LE PÉRIMÈTRE DU POUVOIR DE COLLECTE D'INFORMATIONS DE L'ACPR

A. LES PRESTATAIRES TIERS DE SERVICES FONDÉS SUR LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION SONT INCLUS DANS LE PÉRIMÈTRE ACTUEL DU POUVOIR DE COLLECTE D'INFORMATIONS DE L'ACPR

La rédaction actuelle de l'article L. 612-24 du code monétaire et financier consacre la compétence du SGACPR pour demander toute information nécessaire à l'accomplissement de ses missions aux tiers auprès desquels un assujetti au contrôle prudentiel de l'ACPR a externalisé « des fonctions ou des activités opérationnelles ». Ce périmètre à caractère général inclut dans le champ du pouvoir de collecte d'informations de l'ACPR l'ensemble des prestataires tiers répondant au critère d'externalisation. Par suite, les prestataires de services TIC sont déjà couverts par la rédaction actuelle de l'article L. 612-24. Le fait de mentionner une catégorie spécifique de prestataires tiers risquerait, par un effet d'*a contrario*, de fragiliser cette rédaction large qui permet d'inclure l'ensemble des prestataires dans le cadre d'une externalisation.

B. LA MODIFICATION PROPOSÉE DU CODE MONÉTAIRE ET FINANCIER SE TRADUIRAIT PAR UNE COMPLEXIFICATION DU DROIT SANS MODIFICATION SUBSTANTIELLE DES DISPOSITIONS APPLICABLES

La modification proposée par l'article 53 du projet de loi n'est pas opportune dans la mesure où elle aurait pour effet de complexifier la rédaction de l'article L. 612-24 du code monétaire et financier sans modifier substantiellement le droit applicable.

En premier lieu, l'ajout d'une référence spécifique au règlement DORA dans des dispositions codifiées du droit national a pour effet, en dehors du risque d'effet d'a contrario mentionné ci-dessus, de réduire l'accessibilité

[1] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

du droit en complexifiant la rédaction de l'article L. 612-24 du code monétaire et financier. Il a également pour effet de rendre nécessaire une actualisation de cette référence en cas d'évolution du droit de l'Union.

En second lieu, les prestataires de services TIC sont déjà inclus dans la rédaction actuelle de l'article L. 612-24 du code monétaire et financier qui inclus l'ensemble des prestataires dans le cadre d'une externalisation. L'absence de portée effective de cet article est, du reste, évoquée par le Gouvernement dans l'étude d'impact du projet de loi qui souligne que la modification proposée « ne devrait pas avoir d'impact majeur par rapport à la situation existante »[1].

La commission spéciale a donc adopté l'amendement COM-130 du rapporteur Michel Canévet visant à supprimer cet article.

Décision de la commission : la commission spéciale a supprimé cet article.

[1] *Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, étude d'impact, p. 524.*

Article 54

Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement

Le présent article prévoit de mettre à jour l'encadrement des procédures de redressement et de résolution applicables aux établissements de crédit et entreprises d'investissement en matière de planification des mesures de résolution pour assurer la prise en compte de la résilience opérationnelle numérique en cas de défaillance.

L'article prévoit à ce titre, en transposant les obligations prévues par la directive DORA, que les plans de résolution des établissements doivent préciser les modalités de prise en compte de la résilience opérationnelle numérique et décrire les réseaux et systèmes d'information nécessaires à la continuité des processus opérationnels de l'établissement.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : LES ÉTABLISSEMENTS DE CRÉDITS ET LES ENTREPRISES D'INVESTISSEMENT SONT SOUMIS À UN RÉGIME SPÉCIFIQUE EN MATIÈRE DE PROCÉDURES DE REDRESSEMENT ET DE RÉSOLUTION FIXÉ PAR LE DROIT DE L'UNION

A. LA DIRECTIVE « BRRD » DU 15 MAI 2014 FIXE UN CADRE EUROPÉEN EN MATIÈRE DE PROCÉDURE DE REDRESSEMENT ET DE RÉSOLUTION DES ÉTABLISSEMENTS DE CRÉDIT ET DES ENTREPRISES D'INVESTISSEMENT

La directive 2014/59/UE du 15 mai 2024 concernant les règles pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement[1], ou directive « BRRD »[2], fixe un régime harmonisé au sein de l'Union en matière de redressement et de résolution dans le secteur bancaire.

Adoptée postérieurement à la crise économique et financière de 2008 dans le cadre de laquelle plusieurs États membres de l'Union sont intervenus financièrement pour soutenir des banques en difficulté, la directive BRRD a pour but d'éviter l'occurrence de renflouement externe, financé par les

[1] *Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement et modifiant la directive 82/891/CEE du Conseil ainsi que les directives du Parlement européen et du Conseil 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE et 2013/36/UE et les règlements du Parlement européen et du Conseil (UE) n ° 1093/2010 et (UE) n ° 648/2012.*

[2] *Bank Recovery and Resolution Directive (BRRD).*

contribuables, en prévoyant des mécanismes de renflouement interne, dont le coût est supporté en priorité par les actionnaires et les créanciers des établissements bancaires concernés.

À ce titre, la directive prévoit notamment un volet préventif dans le cadre duquel chaque établissement doit établir un plan de redressement et un plan de résolution qui définissent les mesures qui pourront être prise en cas de difficultés financières.

En particulier, l'article 10 prévoit que l'autorité de résolution établisse, pour chaque établissement, un plan de résolution qui définit les mesures pouvant être prises en cas de déclenchement d'une procédure de résolution. Le 7 de l'article 10 dresse une liste d'éléments qui doivent figurer dans le plan de résolution dont une démonstration de la façon dont les fonctions critiques et les activités fondamentales pourraient être séparées des autres fonctions (c) et une description des principaux systèmes et opérations nécessaires à la continuité des processus opérationnels de l'établissement (q).

B. LE RÉGIME DE REDRESSEMENT ET DE RÉSOLUTION DES ÉTABLISSEMENTS DE CRÉDIT ET DES ENTREPRISES D'INVESTISSEMENT, NOTAMMENT EN MATIÈRE DE PLANIFICATION DES MESURES DE RÉSOLUTION, A ÉTÉ TRANSPOSÉ EN DROIT NATIONAL DANS LE CODE MONÉTAIRE ET FINANCIER

Le cadre européen de redressement et de résolution des établissements financiers a notamment été transposé en droit national par l'ordonnance du 20 août 2015 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière[1].

En particulier, en matière d'établissement des plans préventifs de résolution, l'article L. 613-38 du code monétaire et financier prévoit l'établissement par le collège de résolution d'un plan préventif qui prévoit les mesures de résolution applicables et comprend plusieurs éléments dont une liste est fixée au III de l'article.

L'article L. 613-38 prévoit à ce titre que les plans de résolution comprennent notamment d'une part « un descriptif des modalités selon lesquelles les fonction critiques et activités fondamentales pourraient être juridiquement et économiquement dissociées des autres fonction » en assurant la continuité de l'activité en cas de défaillance (3°) et d'autre part une description des principaux systèmes et opérations permettant d'assurer la continuité des processus opérationnels de l'établissement (17°).

---

[1] *Ordonnance n° 2015-1024 du 20 août 2015 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière financière.*

C. LA DIRECTIVE « DORA » DU 14 DÉCEMBRE 2022 A MIS À JOUR LE CADRE DE REDRESSEMENT ET DE RÉSOLUTION DES ÉTABLISSEMENTS BANCAIRES EN MATIÈRE DE PLANIFICATION DES MESURES DE RÉSOLUTION POUR TENIR COMPTE DE LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DES ÉTABLISSEMENTS

La directive (UE) 2022/2556 du 14 décembre 2022[1], ou « directive DORA »[2], prévoit plusieurs dispositions de mise à jour de la directive BRRD.

À ce titre, l'article 5 de la directive DORA a actualisé le cadre fixé par la directive BRRD.

En particulier, le 7 de l'article 10 de la directive BRRD, qui dresse la liste des éléments que doivent comprendre les plans de résolution, a été mis à jour par la directive DORA.

En premier lieu, le c du 7 est mis à jour pour prévoir que le plan de résolution comprend une démonstration de la façon dont les fonctions critiques et les activités fondamentales peuvent être séparées des autres fonctions en assurant non seulement la continuité des activités fondamentales mais également « la résilience opérationnelle numérique » en cas de défaillance de l'établissement.

En second lieu, le q du 7 est mis à jour pour prévoir que le plan de résolution comprend une description des principaux systèmes et opérations garantissant la continuité des processus opérationnels de l'établissement, y compris des réseaux et systèmes d'information visés dans le règlement DORA[3].

II. LE DISPOSITIF PROPOSÉ : LE PROJET DE LOI TRANSPOSE DANS LE DROIT NATIONAL LA MISE À JOUR, EN MATIÈRE DE PLANIFICATION DES MESURES DE RÉSOLUTION, DU CADRE DE REDRESSEMENT ET DE RÉSOLUTION DES ÉTABLISSEMENTS BANCAIRES

L'article 54 du projet de loi transpose la mise à jour du régime de redressement et de résolution des établissements bancaires en matière de planification des mesures de résolution.

En premier lieu, le 1° de l'article 54 modifie le 3° du III de l'article L. 613-38 du code monétaire et financier pour prévoir que les plans de résolution

---

[1] *Directive (UE) 2022/2556 du parlement européen et du conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Digital Operational Resilience Act.*

[3] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

comprennent un descriptif des modalités de séparation des activités fondamentales et des autres activités en assurant non seulement la continuité des activités fondamentales mais également « la résilience opérationnelle numérique ».

En second lieu, le 2° de l'article 54 modifie le 17° du III de l'article L. 613-38 du code monétaire et financier pour prévoir que les plans de résolution comprennent une description des principaux systèmes et opérations nécessaires à la continuité des processus opérationnels de l'établissement, « y compris des réseaux et systèmes d'information » visés dans le règlement DORA[1].

III. LA POSITION DE LA COMMISSION SPÉCIALE : L'APPLICATION DU CADRE ACTUALISÉ DE REDRESSEMENT ET DE RÉSOLUTION EN MATIÈRE DE PLANIFICATION DES MESURES DE RÉSOLUTION AUX ÉTABLISSEMENTS DE CRÉDIT ET AUX ENTREPRISES D'INVESTISSEMENT RÉPOND À LA NÉCESSITÉ DE TRANSPOSER LE DROIT DE L'UNION

La mise à jour des obligations applicables aux établissements de crédit et aux entreprises d'investissement en matière de planification des meures de résolution correspond à la transposition de la directive DORA en droit national par la modification du code monétaire et financier. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[2]. Par suite, la mise à jour du code monétaire et financier prévue par cet article est opportune.

Décision de la commission : la commission spéciale a adopté cet article sans modification.

---

[1] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

[2] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 55

Extension de la liste des autorités habilitées à s'échanger des informations

Le présent article prévoit d'intégrer l'ACPR et la Banque de France dans la liste des autorités habilitées à s'échanger des informations utiles à leurs missions dans le domaine de la sécurité des systèmes d'informations.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : SEULES L'AMF ET L'ANSSI SONT HABILITÉES À ÉCHANGER LEURS INFORMATIONS EN MATIÈRE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Le 4ème alinéa du II de l'article L. 631-1 du code monétaire et financier (CMF) prévoit que **l'Autorité des marchés financiers (AMF) et l'autorité nationale en charge de la sécurité des systèmes d'information (ANSSI)** sont habilitées à se communiquer les informations utiles à l'exercice de leurs missions dans le domaine de la sécurité des systèmes d'information.

Ces **communications d'informations** peuvent prendre la forme de rapports d'incidents ou de menaces cyber, de réunions de crise ou de réunions périodiques de portée plus générale sur l'état de la menace cyber. **L'AMF et l'ANSSI** sont en contact continu et participent à **plusieurs comités et cadres d'échanges d'information** (réseau des CSIRT[1], EU-SCICF[2], Groupe de place Robustesse[3]…)

II. LE DISPOSITIF PROPOSÉ : LE PRÉSENT ARTICLE COMPLÈTE LA LISTE DES AUTORITÉS HABILITÉES À S'ÉCHANGER DES INFORMATIONS EN Y AJOUTANT L'ACPR ET LA BANQUE DE FRANCE

L'article 49 du **règlement DORA** prévoit que les autorités nationales de supervision financière[4] **doivent coopérer étroitement entre elles** et

[1] Computer Secruity Incident Response Team. *On compte aujourd'hui en France près d'une centaine de ces équipes qui sont nommées CSIRT ou CERT (*Computer Emergency Response Team*).*

[2] Cyber Incident Coordination Framework. *Il s'agit du cadre paneuropéen de coordination des incidents cybernétiques systémiques (EU-SCICF)*

[3] *Créé en 2005 à l'initiative de la Banque de France, le groupe de place Robustesse (GPR) a pour mission de renforcer la résilience opérationnelle de la Place financière de Paris, en s'assurant de la capacité du système financier à faire face à des chocs opérationnels affectant ses fonctions critiques.*

[4] *Ces autorités sont les « autorités compétentes » prévues à l'article 46 du règlement DORA.*

échanger des informations afin de s'acquitter de leurs missions, notamment leurs pouvoirs de surveillance, d'enquête et de sanction prévus à l'article 50 du règlement DORA. Aux termes de **l'article 19 du règlement DORA**, les entités financières doivent notifier les incidents majeurs liés aux TIC auprès des **autorités compétentes nationales**. S'agissant **des prestataires de services de paiement**, les notifications d'incidents doivent ainsi en France être transmises **à la Banque de France et à l'ACPR**.

Dès lors, le présent article prévoit **de compléter le II de l'article L. 631-1 du code monétaire et financier** afin d'ajouter la **Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR)** dans la liste des autorités habilitées à s'échanger des informations.

III. LA POSITION DE LA COMMISSION : UN COMPLÉMENT NÉCESSAIRE POUR GARANTIR LE PARTAGE D'INFORMATIONS ENTRE TOUTES LES AUTORITÉS COMPÉTENTES

L'ajout envisagé par le présent article est indispensable du point de vue juridique, afin de **lever le secret professionnel**, sanctionné pénalement, qui pèse sur l'ACPR et la Banque de France. Le présent article permet d'**autoriser l'ACPR et la Banque de France à communiquer leurs informations confidentielles à l'ANSSI dans le cadre de leurs missions liée à DORA**.

Ces échanges sont nécessaires, par exemple pour coordonner les réponses à incidents, partager des informations sur les menaces cyber ou organiser des tests d'intrusion fondées sur la menace.

Décision de la commission : la commission a adopté cet article sans modification

Article 56

Adaptations pour rendre applicables en outre-mer les modifications du code monétaire et financier prévues par le présent projet de loi

Le présent article prévoit de rendre applicables en Nouvelle-Calédonie, en Polynésie française et dans les îles de Wallis-et-Futuna les modifications des articles du code monétaire et financier introduites par les articles 43 à 55 du projet de loi.

Le rapporteur Michel Canévet a déposé un amendement COM-131 pour supprimer deux modifications rendues superflues par la publication de l'ordonnance ***du 15 octobre 2024 relative aux marchés des crypto-actifs et pour corriger une erreur de référence, adopté par la commission spéciale.***

La commission a adopté cet article ainsi modifié.

I. LE DROIT EXISTANT : EN NOUVELLE-CALÉDONIE, EN POLYNÉSIE FRANÇAISE ET À WALLIS-ET-FUTUNA, TOUTE CRÉATION OU MODIFICATION DU CODE MONÉTAIRE ET FINANCIER DOIT ÊTRE RENDUE APPLICABLE PAR MENTION EXPRESSE

Les collectivités du Pacifique relevant de **l'article 74 de la Constitution** (**Polynésie française**, **îles Wallis-et-Futuna**) et la **Nouvelle-Calédonie**, qui relève **de l'article 77 de la Constitution,** sont soumises au **principe de spécialité législative**. Suivant ce principe, les lois et règlements n'y sont applicables que dans **les matières relevant statutairement de la compétence de l'État et sur mention expresse d'applicabilité**.

Dans ces trois collectivités, **l'État est compétent en matière bancaire et financière**. Les modifications du **code monétaire et financier** ne sont donc applicables que sur **mention expresse**.

Il est alors nécessaire de prévoir une **rédaction dite « compteur Lifou** »[1]. Les « compteurs Lifou » constituent une technique de rédaction des dispositions d'application outre-mer des textes législatifs et réglementaires visant à assurer la traçabilité de l'extension des dispositions normatives et de leurs modifications pour les **collectivités soumises au principe de spécialité législative.**

Suivant cette technique, la disposition du texte applicable dans une collectivité soumise au **principe de spécialité** est signalée par la mention que

[1] *Dans sa décision d'assemblée du 9 février 1990, dite « Élections municipales de Lifou », le Conseil d'État a jugé qu'une loi ou qu'un décret modifiant le droit en vigueur dans une collectivité d'outre-mer doit comporter la mention expresse d'application outre-mer. À défaut, le texte antérieur demeure en vigueur dans le territoire concerné.*

ce texte est désormais applicable « *dans sa rédaction résultant de la loi (ou du décret) n° ...du ...* ». Chaque **modification ultérieure** est opérée par une **modification de la référence du texte**. Dans les **codes figurent un tableau** indiquant, en deux colonnes, pour chaque collectivité concernée, les dispositions du code **qui sont étendues** et la **rédaction** dans laquelle elles sont applicables.

Récemment, la **loi du 13 juillet 2023** ratifiant les ordonnances relatives à la partie législative du livre VII du code monétaire et financier et portant diverses dispositions relatives à l'outre-mer[1] a ainsi rendu applicables dans ces trois territoires, via des mentions expresses, des **modifications intervenues dans le code monétaire et financier**.

II. LE DISPOSITIF PROPOSÉ : LE PRÉSENT ARTICLE PRÉVOIT DE RENDRE APPLICABLES EN NOUVELLE-CALÉDONIE, EN POLYNÉSIE FRANÇAISE ET A WALLIS-ET-FUTUNA LES MODIFICATIONS INTRODUITES PAR LES ARTICLES 43 À 55 DU PROJET DE LOI

Suivant la technique dite du « compteur Lifou », le présent article prévoit de modifier de **nombreuses dispositions du Livre VII du code monétaire et financier consacré aux dispositions relatives à l'outre-mer**, afin de rendre applicables les modifications apportées par le projet de loi au code monétaire et financier.

Le présent article permet de rendre applicables en Nouvelle-Calédonie, en Polynésie française et à Wallis-et-Futuna les modifications du code monétaire et financier prévues aux articles **43 à 55 du projet de loi.**

Dans le détail, sont concernées les articles L. 712-7, L. 752-10, L.754-8, L. 761-1, L. 762-3, L. 763-3, L. 764-3, L. 762-4, L. 763-4, L. 764-4, L. 771-1, L. 781-1, L. 773-5, L. 774-5, L. 775-5, L. 773-6, L. 774-6, L. 775-6, L. 773-21, L. 774-21, L. 775-15, L. 773-30, L. 774-30 et L. 775-24 du code monétaire et financier. Pour les articles concernés, les modifications sont opérées en **actualisant avec la référence du présent projet de loi les tableaux établis au titre du « compteur Lifou »**.

---

[1] *Loi n° 2023-594 du 13 juillet 2023 ratifiant les ordonnances relatives à la partie législative du livre VII du code monétaire et financier et portant diverses dispositions relatives à l'outre-mer*

III. LA POSITION DE LA COMMISSION : DES MENTIONS EXPRESSES NÉCESSAIRES POUR ASSURER L'APPLICATION DES ARTICLES 43 À 55 DANS CES 3 COLLECTIVITÉS ULTRAMARINES MAIS DES RÉFÉRENCES ERRONÉES À SUPPRIMER

Le présent article permet **d'assurer l'application en Nouvelle-Calédonie, en Polynésie française et à Wallis-et-Futuna** des modifications du CMF introduites par les articles 43 à 55 du projet de loi.

Si ces modifications sont nécessaires, certaines d'entre elles **ne sont pas utiles ou reposent sur des références erronées**.

Ainsi, le présent article prévoit de modifier **l'article L. 761.1 du code monétaire et financier** afin d'y ajouter la référence au règlement DORA du 14 décembre 2022[1]. Or **cette mention figure déjà dans cet article**, à la suite de la publication de l'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés des crypto-actifs.

De même, le présent article prévoit de modifier les **articles L. 771-1 et L. 781-1 du code monétaire et financier** afin d'y ajouter la référence au règlement DORA du 14 décembre 2022. Or, **cette mention figure déjà dans cet article**, à la suite de la publication de l'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés des crypto-actifs.

Par ailleurs, le présent article prévoit de modifier l'article L. 785-4 du code monétaire et financier afin de préciser que l'article L. 613-38 est applicable dans les 3 collectivités dans sa rédaction résultant du présent projet de loi, et non plus dans celle issue de l'ordonnance n° 2020-1636 du 21 décembre 2020. Or il s'agit d'une **erreur de référence**, **l'article L. 785-4 ne renvoyant pas à cet article**. L'article à modifier est **l'article L. 785-3 du code monétaire et financier**.

Dès lors, l'amendement **n° COM-131** du rapporteur Michel Canévet, adopté par la commission spéciale, propose des modifications afin de **corriger ces erreurs de rédaction**.

Décision de la commission : la commission a adopté cet article ainsi modifié.

---

[1] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011.*

CHAPITRE II
DISPOSITIONS MODIFIANT LE CODE DES ASSURANCES

Article 57

Nouvelles obligations pour les entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Le présent article prévoit de modifier l'article L. 354-1 du code des assurances pour intégrer les nouvelles obligations applicables aux entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information, introduites par le règlement et la directive dits « DORA ».

Les fonds de retraite professionnelle supplémentaire, auxquels l'article L. 354-1 du code des assurances est applicable, seront également assujettis à ces nouvelles obligations.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : UN ENCADREMENT EUROPÉEN DES ORGANISMES D'ASSURANCE ET DE RÉASSURANCE

A. LES ENTREPRISES D'ASSURANCE ET DE RÉASSURANCE SONT SOUMISES PAR LE DROIT EUROPÉEN À DES OBLIGATIONS PRUDENTIELLES

Les entreprises d'assurance et de réassurance font l'objet d'un encadrement par le droit de l'Union européenne. En l'état du droit, cet encadrement est fixé par la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009, dite « Solvabilité II »[1]. La directive, entrée en vigueur en 2016, **a permis une clarification et une modernisation du droit européen des assurances**. Elle constitue à ce titre un « quasi-code européen des assurances »[2] et a été amendée à la marge par la directive dite « Omnibus II »[3], principalement au titre des exigences quantitatives de fonds propres qu'elle prévoit.

---

[1] *Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[2] *Certains domaines, comme la distribution des produits d'assurance ou l'assurance responsabilité civile demeurent exclus de cette compilation.*

[3] *Directive 2014/51/UE du Parlement européen et du Conseil du 16 avril 2014 modifiant les directives 2003/71/CE et 2009/138/CE et les règlements (CE) n° 1060/2009, (UE) n° 1094/2010 et (UE) n° 1095/2010 en ce qui concerne les compétences de l'Autorité européenne de surveillance*

La directive « Solvabilité II » **a permis de réviser le cadre prudentiel des activités d'assurance et de réassurance au sein de l'Union européenne, afin de garantir la solvabilité des organismes d'assurance**, définie comme leur capacité financière à faire face à leurs engagements compte tenu des risques auxquels ils sont exposés. Ce cadre prudentiel, inspiré de la réglementation prudentielle applicable aux banques, dite « Bâle III », **repose sur trois piliers principaux**.

Un premier pilier a instauré **des exigences quantitatives concernant le capital des organismes**. Chaque organisme d'assurance se voit fixer des niveaux de fonds propres à respecter, selon une approche économique fondée sur le risque. Ces fonds propres permettent de couvrir deux niveaux d'exigence de capital :

- d'une part, le capital minimal requis (*Minimum Capital Requirement* – MCR), définis comme le niveau minimal de fonds propres en-dessous duquel l'intervention de l'autorité de contrôle est automatique ;

- d'autre part, le capital de solvabilité requis (*Solvency Capital Requirement* – SCR), défini comme le capital cible nécessaire pour absorber un choc provoqué par un risque majeur. Calculé annuellement et notifié aux autorités de contrôle, il doit permettre à l'entreprise d'assurer pendant un an ses engagements à 95,5 %. Le SCR est calculé selon une formule standard prévue par la directive « Solvabilité II » et le règlement délégué de la Commission européenne du 10 octobre 2014[1] ou selon un modèle interne complet ou partiel.

Un deuxième pilier a mis en place, pour les organismes d'assurance et de réassurance, **des exigences qualitatives en matière de gouvernance** (cf. encadré *infra*).

(Autorité européenne des assurances et des pensions professionnelles) et de l'Autorité européenne de surveillance (Autorité européenne des marchés financiers)

[1] *Règlement délégué (UE) 2015/35 de la Commission du 10 octobre 2014 complétant la directive 2009/138/CE du Parlement européen et du Conseil sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II).*

Les exigences qualitatives en matière de gouvernance pour les organismes d'assurance et de réassurance

En complément des exigences quantitatives de fonds propres, la directive « Solvabilité II » a également introduit des exigences qualitatives tenant au système de gouvernance des organismes d'assurance et de réassurance (articles 40 à 50 de la directive). Elle impose à ces entreprise la mise en place d'un « *système de gouvernance garantissant une gestion saine et prudente de l'activité* »[1], fondé sur quatre fonctions : la fonction de gestion des risques, la fonction de conformité, la fonction d'audit interne et la fonction actuarielle. Des exigences d'honorabilité et de compétence sont imposées aux responsables de ces quatre fonctions et aux dirigeants des organismes.

L'article 41 de la directive fixe les principes généraux applicables à ce système de gouvernance. Les assureurs doivent ainsi démontrer qu'ils ont adopté une stratégie de gestion du risque, une structure organisationnelle et opérationnelle appropriée ainsi qu'un système de contrôle interne et une fonction d'audit interne efficaces. Ces contraintes sont toutefois soumises à un principe de proportionnalité et s'appliquent à tous les assureurs selon la nature, l'ampleur et la complexité de leurs opérations.

Les entreprises d'assurance et de réassurance conservent l'entière responsabilité de ces obligations, y compris en cas de sous-traitance.

De plus, dans le cadre de leur système de gestion des risques, les organismes d'assurance et de réassurance doivent procéder annuellement à une évaluation interne des risques et de la solvabilité (*Own Risk and Solvency Assessment* – ORSA) portant sur le besoin global de solvabilité, le respect des exigences de capital et la mesure dans laquelle le profil de risque de l'entreprise s'écarte des hypothèses qui sous-tendent le capital de solvabilité requis[2].

Source : commission des finances d'après la directive « Solvabilité II »

Un troisième pilier a imposé aux entreprises d'assurance et de réassurance **des exigences de transparence à destination du public et du superviseur.** Elles se matérialisent **par la publication d'un rapport annuel sur la solvabilité et la situation financière** et la remise à l'autorité nationale de contrôle et de supervision d'un rapport régulier.

En droit interne, les obligations introduites par la directive « Solvabilité II » ont été transposées par l'ordonnance n° 2015-378 du 2 avril 2015[3] au titre V du livre III du code des assurances, qui regroupe ainsi les principales dispositions prudentielles s'appliquant aux entreprises d'assurance. Plus précisément, les exigences qualitatives en matière de gouvernance applicables aux organismes d'assurance et de réassurance ont

[1] *Article 41 de la directive « Solvabilité II ».*
[2] *Article 45 de la directive « Solvabilité II ».*
[3] *Ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

été introduites dans ce même code au sein du chapitre IV du titre V du livre III. En particulier :

- l'article L. 354-1 du code des assurances dispose que les entreprises d'assurance et de réassurance mettent en place un « *système de gouvernance garantissant une gestion saine et prudente de leur activité et faisant l'objet d'un réexamen interne régulier* », **comprenant les quatre fonctions** de gestion des risques, de vérification de la conformité, d'audit et actuarielle introduites par la directive « Solvabilité II ». Cet article précise que les entreprises **élaborent des politiques écrites relatives à la gestion des risques, au contrôle interne, à l'audit interne et, si besoin, à l'externalisation** ;

- l'article L. 354-2 du même code précise les **obligations attenantes à la mise en place d'un système de gestion des risques** ;

- l'article L. 354-3 du même code précise les éléments relatifs à l'externalisation, **les entreprises d'assurance et de réassurance conservant l'entière responsabilité du respect des obligations qui leur incombent lorsqu'elles y ont recours.**

B. LE RÈGLEMENT DIT « DORA » ET LA DIRECTIVE DU MÊME NOM INTRODUISENT DE NOUVELLES OBLIGATIONS POUR LES ENTREPRISES D'ASSURANCE ET DE RÉASSURANCE EN MATIÈRE DE GOUVERNANCE

La directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022, dite « DORA »[1], **intègre dans la directive « Solvabilité II » les nouvelles exigences introduites par le règlement (UE) 2022/2554** du Parlement européen et du Conseil du 14 décembre 2022, dit règlement « DORA »[2], et applicables aux organismes d'assurance et de réassurance.

L'article 2 de la directive « DORA » vient ainsi modifier l'article 41 paragraphe 4 de la directive « Solvabilité II », relatif aux obligations de gouvernance et de gestion des risques, pour indiquer que les organismes d'assurance et de réassurance « *utilisent des systèmes, des ressources et des procédures appropriés et proportionnés et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil* »[3]. Le second pilier de la directive « Solvabilité II » **se voit donc complété d'un volet relatif à la gestion des risques relatifs aux technologies de l'information et de la communication**.

---

[1] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[2] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

[3] *Article 2 de la directive « DORA ».*

Dans le même sens, l'article 8 de la directive « DORA » modifie le paragraphe 5 de l'article 21 de la directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016[1] pour prévoir l'application de cette obligation aux institutions de retraite professionnelle.

Cette obligation de mise en place et de gestion des réseaux et des systèmes d'information conformément au règlement « DORA » **recouvre quatre volets.**

Premièrement, **les entités financières concernées sont tenues de mettre en place un cadre de gouvernance et de contrôle interne** garantissant « *une gestion efficace et prudente du risque lié aux TIC (…) en vue d'atteindre un niveau élevé de résilience opérationnelle numérique* »[2].

Deuxièmement, le règlement « DORA » impose aux entités financières **une standardisation des mécanismes de détection, classification et notification des incidents liés aux TIC**. Ces entités doivent notamment notifier à leur autorité compétente, en l'espèce l'ACPR, les incidents majeurs liés aux TIC.

Troisièmement, **les entités financières entrant dans le champ d'application du règlement « DORA » doivent réaliser des tests de résilience opérationnelle numérique**[3]. Ce programme de tests vise à évaluer l'état de préparation de l'entreprise pour faire face aux risques liés aux technologies de l'information et de la communication, à recenser les faiblesses, défaillances et lacunes en matière de résilience numérique et à mettre en œuvre rapidement des mesures correctives.

Quatrièmement, ces entités doivent mettre en place des mesures pour anticiper les risques liés au recours à des prestataires de tiers de services TIC.

En droit interne, la prise en compte de ces évolutions du cadre européen implique une mise à jour des dispositions du code des assurances et, plus spécifiquement, de son article L. 354-1 qui rassemble les dispositions relatives au système de gouvernance des entreprises d'assurance et de réassurance.

II. LE DISPOSITIF PROPOSÉ : UNE MODIFICATION DU CODE DES ASSURANCES VISANT À PRENDRE EN COMPTE LES NOUVELLES OBLIGATIONS ISSUES DE LA DIRECTIVE DITE « DORA »

Le présent article modifie l'article L. 354-1 du code des assurances à deux occurrences.

---

[1] *Directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016 concernant les activités et la surveillance des institutions de retraite professionnelle (IRP).*
[2] *Article 5 du règlement « DORA ».*
[3] *Article 24 du règlement « DORA ».*

En premier lieu, il opère une précision matérielle à la première phrase du troisième alinéa **en indiquant que l'externalisation opérées par les entreprises d'assurance renvoie à une définition figurant au 13° de l'article L. 310-3 du code des assurances**. Ce dernier dispose que l'externalisation désigne « *un accord, quelle que soit sa forme, conclu entre une entreprise et un prestataire de services, soumis ou non à un contrôle, en vertu duquel ce prestataire de services exécute, soit directement, soit en recourant lui-même à l'externalisation, une procédure, un service ou une activité, qui serait autrement exécuté par l'entreprise elle-même* ». Cette précision reprend la rédaction des articles L. 211-12 du code de la mutualité et L. 931-7 du code de la sécurité sociale, miroirs de l'article L. 354-1 du code des assurances.

En second lieu, le présent article complète la seconde phrase du quatrième alinéa de l'article L. 354-1 du code des assurances pour indiquer que les entreprises d'assurance et de réassurance **mettent en place et gèrent des réseaux et des systèmes d'information conformément aux exigences du règlement « DORA ».** Cette rédaction reprend celle retenue par le premier paragraphe de l'article 2 de la directive « DORA » pour modifier le paragraphe 4 de l'article 41 de la directive « Solvabilité II », dont l'article L. 354-1 du code des assurances assure la transposition en droit interne.

Dès lors que l'article L. 385-5 du code des assurances dispose que le chapitre IV du titre V du livre III du même code, dans lequel s'inscrit l'article L. 354-1, **s'applique aux fonds de retraite professionnelle supplémentaire, la présente modification s'appliquera également à ces organismes.**

III. LA POSITION DE LA COMMISSION SPÉCIALE : UNE TRANSPOSITION NÉCESSAIRE DES EXIGENCES DU RÉGIME « DORA » DANS LE CODE DES ASSURANCES

Dès lors que la directive dite « DORA » prévoyait une modification du régime « Solvabilité II », **une adaptation de l'article L. 354-1 du code des assurances, qui transpose les exigences de ce régime en matière de gouvernance, apparaissait incontournable**. Le choix du Gouvernement de reproduire la rédaction retenue par la directive permet d'assurer une transposition *a minima*. Comme a pu le noter le Conseil d'État dans son avis sur le présent projet de loi, ce choix de transposition « *conduit à ce que certaines dispositions nationales prévoient des obligations identiques à celles instituées par le règlement « DORA », en les définissant par référence à ce dernier* »[1]. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre

[1] *Conseil d'État, Section de l'administration, Section des finances, Avis sur un projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier, n° 408329, 6 juin 2024.*

commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

S'agissant de la perception du règlement et de la directive « DORA » par les entreprises du secteur assurantiel, **ces dernières ont accueilli positivement les obligations introduites par ces textes**. Sans disposer de données compilées, les entités du secteur sont affectées par les cyber-attaques soit directement, soit par leurs partenaires. Si elles ont adopté des mesures techniques pour se prémunir de ces agressions, **les exigences du paquet « DORA » devraient permettre de consolider et de formaliser les pratiques dans un cadre proportionné à chaque entreprise.**

La fédération France Assureurs, sollicitée par le rapporteur, **a indiqué la mise en conformité des organismes d'assurance avait fortement mobilisé ces derniers**[2]. Selon les données présentées dans l'étude d'impact du présent article, les coûts induits par la mise en œuvre de DORA seraient évalués, en coûts de projet, à 6 millions d'euros sur 2024-2025 et à 40 millions d'euros sur 2024-2027 et, en coûts opérationnels, entre 700 000 euros et 3 millions d'euros. Les entreprises du secteur, outre ces coûts d'adaptation techniques, ont également eu recours à des cabinets de conseil pour un accompagnement dans les procédures DORA.

La mise en œuvre des exigences du cadre « DORA » dépendra en grande partie des compléments apportés par les normes techniques règlementaires (RTS) et les normes de mise en œuvre (ITS) et par les orientations fixées par les trois autorités européennes de supervision, en cours de discussion. **À ce titre, le rapporteur Michel Canévet sera attentif à l'organisation adoptée par l'Autorité de contrôle prudentiel et de résolution dans l'application du contrôle des exigences du cadre « DORA ».**

Décision de la commission spéciale : la commission spéciale a adopté cet article sans modification.

---

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

[2] *Réponses de France Assureurs au questionnaire du rapporteur.*

Article 58

Extension aux groupes d'assurance des nouvelles obligations de gouvernance des risques liés à l'utilisation des systèmes d'information

Le présent article prévoit de modifier l'article L. 356-18 du code des assurances pour intégrer les nouvelles obligations applicables aux entreprises têtes de groupes d'assurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information, introduites par le règlement et la directive dits « DORA ».

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : UN ENCADREMENT EUROPÉEN DES ORGANISMES D'ASSURANCE ET DE RÉASSURANCE S'APPLIQUANT *MUTATIS MUTANDIS* AU NIVEAU DU GROUPE

A. LES ENTREPRISES D'ASSURANCE ET DE RÉASSURANCE SONT SOUMISES PAR LE DROIT EUROPÉEN À DES OBLIGATIONS PRUDENTIELLES DONT L'APPLICATION EST ÉTENDUE AU NIVEAU DU GROUPE

Comme indiqué dans le commentaire de l'article 57 du présent projet de loi, **les entreprises d'assurance et de réassurance font l'objet d'un encadrement par le droit de l'Union européenne,** fixé par la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009, dite « Solvabilité II »[1]. Entrée en vigueur en 2016, cette directive **a permis une clarification et une modernisation du droit européen des assurances**. Elle a fixé **un cadre prudentiel organisé autour de trois piliers :** des exigences quantitatives de fonds propres, des exigences qualitatives en matière de gouvernance et des exigences de transparence à destination du public et du superviseur[2].

S'agissant des exigences qualitatives en matière de gouvernance[3], l'article 246 de la directive « Solvabilité II » **prévoit qu'elles s'appliquent de manière équivalente aux groupes d'assurance**. Comme le souligne l'étude d'impact du présent projet de loi « *les règles de gouvernance des groupes sont pour l'essentiel mises en œuvre par l'entreprise tête de groupe* ». Ces entreprises têtes de groupes **peuvent être soit des entreprises d'assurance ou de réassurance**

[1] *Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[2] *Pour des développements plus approfondis sur la directive « Solvabilité II », le lecteur pourra se reporter au commentaire de l'article 57.*

[3] *Prévues au sein de la section 2 du chapitre IV du titre 2 de la directive.*

participantes dans une entreprises d'assurance ou de réassurance, soit des entreprises mères[1].

En droit interne, les obligations introduites par la directive « Solvabilité II » **ont été transposées par l'ordonnance n° 2015-378 du 2 avril 2015**[2] **au sein du code des assurances**. Les articles L. 356-18 et L. 356-19 du code des assurances transposent l'article 246 de la directive. **Les exigences applicables aux groupes d'assurance en matière de gouvernance sont spécifiées à l'article L. 356-18 du code des assurances**. Les dispositions de cet article dupliquent, pour les groupes d'assurance, la rédaction retenue par l'article L. 354-1 du même code pour les entreprises d'assurance et de réassurance.

Aux termes de l'article L. 356-18, les entreprises participantes et mères doivent donc mettre en place un « *système de gouvernance garantissant une gestion saine et prudente de leur activité et faisant l'objet d'un réexamen interne régulier* », **comprenant les quatre fonctions** de gestion des risques, de vérification de la conformité, d'audit et actuarielle introduites par la directive « Solvabilité II ». Cet article précise que les entreprises participantes et mères **élaborent des politiques écrites relatives à la gestion des risques, au contrôle interne, à l'audit interne et, si besoin, à l'externalisation**.

B. LE RÈGLEMENT DIT « DORA » ET LA DIRECTIVE DU MÊME NOM INTRODUISENT DE NOUVELLES OBLIGATIONS POUR LES ENTREPRISES D'ASSURANCE ET DE RÉASSURANCE EN MATIÈRE DE GOUVERNANCE, ÉGALEMENT APPLICABLES AU NIVEAU DU GROUPE

La directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022, dite « DORA »[3], **intègre dans la directive « Solvabilité II » les nouvelles exigences introduites par le règlement (UE) 2022/2554** du Parlement européen et du Conseil du 14 décembre 2022, dit règlement « DORA »[4], et applicables aux organismes d'assurance et de réassurance.

---

[1] *En droit interne, l'article L. 356-2 du code des assurances définit ces entreprises têtes de groupes comme, d'une part, les* « entreprises participantes dans au moins une entreprise d'assurance, une entreprise de réassurance, une entreprise d'assurance d'un pays tiers ou une entreprise de réassurance d'un pays tiers » *et, d'autre part, comme les entreprises mères de type holding, i.e. une société de groupe d'assurance (SGA), une société de groupe d'assurance mutuelle (SGAM), une union mutualiste de groupe (UMG) ou une société de groupe assurantiel de protection sociale (SGAPS).*

[2] *Ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[3] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[4] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

L'article 2 de la directive « DORA » vient ainsi modifier le paragraphe 4 de l'article 41 de la directive « Solvabilité II », **relatif aux obligations de gouvernance et de gestion des risques**, pour indiquer que les organismes d'assurance et de réassurance « *utilisent des systèmes, des ressources et des procédures appropriés et proportionnés et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil* »[1]. Le second pilier de la directive « Solvabilité II » **se voit donc complété d'un volet relatif à la gestion des risques relatifs aux technologies de l'information et de la communication**[2].

En droit interne, la prise en compte de ces évolutions du cadre européen **implique une mise à jour des dispositions du code des assurances** et, plus spécifiquement, de son article L. 356-18 qui rassemble les dispositions relatives au système de gouvernance des entreprises têtes de groupes d'assurance.

II. LE DISPOSITIF PROPOSÉ : UNE MODIFICATION DU CODE DES ASSURANCES VISANT À PRENDRE EN COMPTE LES NOUVELLES OBLIGATIONS ISSUES DE LA DIRECTIVE DITE « DORA » APPLICABLES AUX GROUPES D'ASSURANCE

Le présent article modifie l'article L. 356-18 du code des assurances à deux occurrences.

En premier lieu, il opère une précision matérielle à la première phrase du troisième alinéa **en indiquant que l'externalisation opérée par les entreprises d'assurance renvoie à une définition figurant au 13° de l'article L. 310-3 du code des assurances**. Cette précision reprend la rédaction des articles L. 211-12 du code de la mutualité et L. 931-7 du code de la sécurité sociale[3].

En second lieu, le présent article complète la seconde phrase du quatrième alinéa de l'article L. 356-18 du code des assurances pour indiquer que les entreprises têtes de groupes d'assurance **mettent en place et gèrent des réseaux et des systèmes d'information conformément aux exigences du règlement « DORA ».** Cette rédaction reprend celle retenue par le premier paragraphe de l'article 2 de la directive « DORA » pour modifier le paragraphe 4 de l'article 41 de la directive « Solvabilité II », dont l'article L. 356-18 du code des assurances assure la transposition en droit interne pour les groupes d'assurance.

---

[1] *Article 2 de la directive « DORA ».*

[2] *Pour des développements sur le contenu des exigences introduites par le règlement « DORA », se référer au commentaire de l'article 57 du présent projet de loi.*

[3] *Un alignement similaire est opéré, pour les entreprises d'assurance et de réassurance, à l'article L. 354-1 du code des assurances par le 1° de l'article 57 du présent projet de loi.*

III. LA POSITION DE LA COMMISSION SPÉCIALE : UNE TRANSPOSITION NÉCESSAIRE DES EXIGENCES DU RÉGIME « DORA » DANS LE CODE DES ASSURANCES POUR LES GROUPES D'ASSURANCE ET DE RÉASSURANCE

De manière similaire au dispositif porté par l'article 57 du présent projet de loi, l'article 58 prévoit une adaptation du code des assurances pour tirer les conséquences de la modification du régime « Solvabilité II » par la directive « DORA ». Le choix du Gouvernement de reproduire la rédaction retenue par la directive permet d'assurer une transposition *a minima*. Cette transposition, qui est nécessaire pour garantir l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

Comme indiqué dans le commentaire de l'article 57, les exigences en matière de gouvernance des risques TIC portées par le paquet « DORA » ont été positivement perçues par le secteur en ce qu'elles permettront de **formaliser et de consolider les mesures prises par les organismes d'assurance pour prévenir les cyber-attaques.**

Décision de la commission spéciale : la commission a adopté cet article sans modification.

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

CHAPITRE III
DISPOSITIONS MODIFIANT LE CODE DE LA MUTUALITÉ

Article 59

Nouvelles obligations pour les unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Le présent article prévoit de modifier le code de la mutualité pour intégrer les nouvelles obligations applicables aux unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information, introduites par le règlement et la directive dits « DORA ».

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : UN ENCADREMENT EUROPÉEN DES ORGANISMES D'ASSURANCE ET DE RÉASSURANCE S'APPLIQUANT AUX UNIONS ET MUTUELLES DU CODE DE LA MUTUALITÉ

A. LES UNIONS ET MUTUELLES DU CODE DE LA MUTUALITÉ SONT SOUMISES PAR LE DROIT EUROPÉEN À DES OBLIGATIONS PRUDENTIELLES

Comme indiqué dans le commentaire de l'article 57 du présent projet de loi, **les entreprises d'assurance et de réassurance font l'objet d'un encadrement par le droit de l'Union européenne,** fixé par la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009, dite « Solvabilité II »[1]. Entrée en vigueur en 2016, cette directive **a permis une clarification et une modernisation du droit européen des assurances**. Elle a fixé **un cadre prudentiel organisé autour de trois piliers :** des exigences quantitatives de fonds propres, des exigences qualitatives en matière de gouvernance et des exigences de transparence à destination du public et du superviseur[2].

En droit interne, les obligations introduites par la directive « Solvabilité II » **ont été transposées par l'ordonnance n° 2015-378 du**

[1] *Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[2] *Pour des développements plus approfondis sur la directive « Solvabilité II », le lecteur pourra se reporter au commentaire de l'article 57.*

2 avril 2015[1] au sein du code des assurances, du code de la mutualité et du code de la sécurité sociale. En effet, en France, les opérations d'assurance peuvent être **pratiquées par trois types d'organismes :** les entreprises d'assurance (dont les sociétés anonymes d'assurance et les sociétés d'assurance mutuelle), les mutuelles et unions régies par le code de la mutualité, et les institutions de prévoyance. Si la transposition de la directive « Solvabilité II » a été l'occasion de regrouper au sein du code des assurances les règles prudentielles applicables aux organismes pratiquant des opérations d'assurance, les dispositions relatives à leur gouvernance ont été maintenues dans les trois codes précités[2].

Au sein du code de la mutualité, l'article 14 de l'ordonnance n° 2015-378 a créé une nouvelle sous-section au chapitre Ier du livre II consacrée **au système de gouvernance applicable aux mutuelles et unions relevant du régime dit « Solvabilité II ».** L'article L. 211-12 du code de la mutualité, dont la rédaction est identique aux articles L. 354-1 du code des assurances et L. 931-7 du code de la sécurité sociale, dispose que les entreprises d'assurance et de réassurance mettent en place un « *système de gouvernance garantissant une gestion saine et prudente de leur activité et faisant l'objet d'un réexamen interne régulier* », **comprenant quatre fonctions** de gestion des risques, de vérification de la conformité, d'audit et actuarielle introduites par la directive « Solvabilité II ». Cet article précise que les entreprises **élaborent des politiques écrites relatives à la gestion des risques, au contrôle interne, à l'audit interne et, si besoin, à l'externalisation.**

B. LE RÈGLEMENT DIT « DORA » ET LA DIRECTIVE DU MÊME NOM INTRODUISENT DE NOUVELLES OBLIGATIONS POUR LES UNIONS ET MUTUELLES DU CODE DE LA MUTUALITÉ EN MATIÈRE DE GOUVERNANCE

La directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022, dite « DORA »[3], **intègre dans la directive « Solvabilité II » les nouvelles exigences introduites par le règlement (UE) 2022/2554** du Parlement européen et du Conseil du 14 décembre 2022, dit règlement « DORA »[4], et applicables aux unions et mutuelles du code de la mutualité.

---

[1] *Ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[2] *Rapport au Président de la République relatif à l'ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II).*

[3] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

[4] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

L'article 2 de la directive « DORA » vient ainsi modifier le paragraphe 4 de l'article 41 de la directive « Solvabilité II », **relatif aux obligations de gouvernance et de gestion des risques**, pour indiquer que les organismes d'assurance et de réassurance « *utilisent des systèmes, des ressources et des procédures appropriés et proportionnés et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil* »[1]. Le second pilier de la directive « Solvabilité II » **se voit donc complété d'un volet relatif à la gestion des risques relatifs aux technologies de l'information et de la communication**[2].

En droit interne, la prise en compte de ces évolutions du cadre européen **implique une mise à jour des dispositions du code de la mutualité** et, plus spécifiquement, de son article L. 211-12 qui rassemble les dispositions relatives au système de gouvernance des unions et mutuelles régies par ce même code.

II. LE DISPOSITIF PROPOSÉ : UNE MODIFICATION DU CODE DE LA MUTUALITÉ VISANT À PRENDRE EN COMPTE LES NOUVELLES OBLIGATIONS ISSUES DE LA DIRECTIVE DITE « DORA » APPLICABLES AUX UNIONS ET MUTUELLES DE CE CODE

Le présent article complète la seconde phrase du quatrième alinéa de l'article L. 211-12 du code de la mutualité pour indiquer que les unions et mutuelles du même code **mettent en place et gèrent des réseaux et des systèmes d'information conformément aux exigences du règlement « DORA ».** Cette rédaction reprend celle retenue par le premier paragraphe de l'article 2 de la directive « DORA » pour modifier le paragraphe 4 de l'article 41 de la directive « Solvabilité II », dont l'article L. 211-12 du code de la mutualité assure la transposition en droit interne pour ces organismes.

III. LA POSITION DE LA COMMISSION SPÉCIALE : UNE ADAPTATION NÉCESSAIRE DU CODE DE LA MUTUALITÉ

De manière similaire aux dispositifs portés par les articles 57 et 58 du présent projet de loi, s'agissant du code des assurances, et l'article 61 pour le code de la sécurité sociale, le présent article prévoit une adaptation du code de la mutualité pour tirer les conséquences de la modification du régime « Solvabilité II » par la directive « DORA ». Le choix du Gouvernement de reproduire la rédaction retenue par la directive permet d'assurer une transposition *a minima*. Cette transposition, qui est nécessaire pour garantir

---

[1] *Article 2 de la directive « DORA ».*

[2] *Pour des développements sur le contenu des exigences introduites par le règlement « DORA », se référer au commentaire de l'article 57 du présent projet de loi.*

l'application d'un cadre commun au sein du marché intérieur, correspond par surcroît à une exigence constitutionnelle[1].

Décision de la commission spéciale : la commission a adopté cet article sans modification.

[1] *Conseil constitutionnel, 10 juin 2004, n° 2004-496 DC, Loi pour la confiance dans l'économie numérique, §7.*

Article 60

Suppression des dispositions redondantes dans le code de la mutualité

Le présent article prévoit de supprimer des redondances dans le code de la mutualité, dans un souci de cohérence et de lisibilité du droit.

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : DEUX DISPOSITIONS REDONDANTES DANS LE CODE DE LA MUTUALITÉ S'AGISSANT DES EXIGENCES DE GOUVERNANCE INTRODUITES PAR LA DIRECTIVE « SOLVABILITÉ II »

L'article L. 212-12 du code de la mutualité rend applicables **aux mutuelles et unions** de ce code les **exigences en matière de gouvernance** prévues par la **directive du 25 novembre 2009, dite « Solvabilité II »**[1]. Comme rappelé dans le commentaire de l'article 59, cet article dispose que le **système de gouvernance** adopté par ces entreprises doit « *garantir une gestion saine et prudente de leur activité et faire l'objet d'un* ***réexamen interne régulier***. Ce système de gouvernance **comprend quatre fonctions** de gestion des risques, de vérification de la conformité, d'audit et actuarielle introduites par la directive « Solvabilité II ». Ces dispositions ont été introduites par l'ordonnance du 2 avril 2015 qui transpose la directive Solvabilité II[2].

Par ailleurs, **l'article L. 212-1 du code de la mutualité** prévoit que « *[l]es dispositions du titre V du livre III […] du code des assurances sont applicables aux mutuelles et unions […]* ». Cela implique que **l'article L. 354-1 du code des assurances** est applicable aux mutuelles et unions du code de la mutualité. Or cet article L. 354-1 du code des assurances porte sur les **exigences de gouvernance** issues de la transposition de la directive Solvabilité II, dans des termes identiques aux dispositions contenues dans l'article L. 212-12 du code de la mutualité.

Autrement dit, actuellement, les mutuelles et unions du code de la mutualité sont **soumises à la fois aux dispositions de l'article L. 211-12 du code de la mutualité et de l'article L. 354-1 du code des assurances** – qui **sont exactement les mêmes**.

---

[1] *Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009, dite « Solvabilité II ».*

[2] *Ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice*

II. LE DISPOSITIF PROPOSÉ : UNE RÉDACTION SIMPLIFIÉE POUR EVITER LA REDONDANCE PRÉSENTE DANS LE CODE DE LA MUTUALITÉ

La redondance des dispositions de **l'article L. 212-12 et L. 212-1 du code de la mutualité** ne pose pas de problème sur le fond mais peut **soulever des difficultés en termes de cohérence et de lisibilité du droit**. A l'occasion de la transposition de la directive DORA, prévue par le présent projet de loi, cette redondance **serait – sans modification du code de la mutualité – reconduite**.

Le présent article prévoit dès lors d'exclure expressément dans **l'article L. 212-1 du code de la** mutualité **l'application de l'article L. 354-1 du code des assurances**. Ce choix s'inspire de la rédaction retenue dans **le code de la sécurité sociale**, son article L. 931-9 précisant que « *Les dispositions du titre V du livre III et de l'article L. 310-12-4 du code des assurances sont applicables aux institutions de prévoyance et unions mentionnées à l'article L. 931-6,* ***à l'exception de l'article L. 354-1 du code des assurances*** **».**

Plus généralement, cette modification permet **d'éviter de procéder par renvoi vers le code des assurances pour définir les exigences de gouvernance applicables aux mutuelles et unions du code de la mutualité**, ceci dans un but de meilleure lisibilité du droit.

III. LA POSITION DE LA COMMISSION : UNE DISPOSITION BIENVENUE POUR PERMETRE UNE MEILLEURE INTELLIGIBILTÉ DE LA LOI

En supprimant une redondance, le présent article permet de **clarifier une disposition du code de la mutualité** et de rendre **plus lisible le droit applicable**. Puisque la transposition de la directive DORA prévue par le présent projet de loi modifie certains des articles concernés, **cette redondance serait reconduite** en l'absence de modification du code de la mutualité.

En ce sens, cette disposition permet de satisfaire **l'objectif à valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi**[1].

Décision de la commission : la commission a adopté cet article sans modification

---

[1] *Conseil constitutionnel, déc. n° 99-421 DC du 16 décembre 1999, Loi portant habilitation du Gouvernement à procéder, par ordonnances, à l'adoption de la partie législative de certains codes, cons. 13.*

CHAPITRE IV
DISPOSITIONS MODIFIANT LE CODE DE LA SÉCURITÉ SOCIALE

Article 61

Nouvelles obligations pour les institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Le présent article prévoit de modifier le code de la sécurité sociale pour intégrer les nouvelles obligations applicables aux institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information, introduites par le règlement et la directive dits « DORA ».

La commission a adopté cet article sans modification.

I. LE DROIT EXISTANT : UN ENCADREMENT EUROPÉEN DES ORGANISMES D'ASSURANCE ET DE RÉASSURANCE S'APPLIQUANT AUX INSTITUTIONS DE PRÉVOYANCE ET UNIONS DU CODE DE LA SÉCURITÉ SOCIALE

A. LES INSTITUTIONS DE PRÉVOYANCE ET UNIONS DU CODE DE LA SÉCURITÉ SOCIALE SONT SOUMISES PAR LE DROIT EUROPÉEN À DES OBLIGATIONS PRUDENTIELLES

Comme indiqué dans le commentaire de l'article 57 du présent projet de loi, **les entreprises d'assurance et de réassurance font l'objet d'un encadrement par le droit de l'Union européenne,** fixé par la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009, dite « Solvabilité II »[1]. Entrée en vigueur en 2016, cette directive **a permis une clarification et une modernisation du droit européen des assurances**. Elle a fixé **un cadre prudentiel organisé autour de trois piliers :** des exigences quantitatives de fonds propres, des exigences qualitatives en matière de gouvernance et des exigences de transparence à destination du public et du superviseur[2].

En droit interne, les obligations introduites par la directive « Solvabilité II » **ont été transposées par l'ordonnance n° 2015-378 du**

[1] *Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[2] *Pour des développements plus approfondis sur la directive « Solvabilité II », le lecteur pourra se reporter au commentaire de l'article 57.*

2 avril 2015[1] **au sein du code des assurances, du code de la mutualité et du code de la sécurité sociale.** En effet, en France, les opérations d'assurance peuvent être pratiquées par trois types d'organismes : les entreprises d'assurance (dont les sociétés anonymes d'assurance et les sociétés d'assurance mutuelle), les mutuelles et unions régies par le code de la mutualité, et les institutions de prévoyance. Si la transposition de la directive « Solvabilité II » a été l'occasion de regrouper au sein du code des assurances les règles prudentielles applicables aux organismes pratiquant des opérations d'assurance, **les dispositions relatives à leur gouvernance ont été maintenues dans les trois codes précités**[2].

Au sein du code de la sécurité sociale, l'article 17 de l'ordonnance n° 2015-378 a créé une nouvelle sous-section au chapitre Ier du titre III du livre IX consacrée **au système de gouvernance applicable aux institutions de prévoyance et unions relevant du régime dit « Solvabilité II ».** L'article L. 931-6 du code de la sécurité sociale prévoie une liste des institutions de prévoyance ou unions relevant de ce régime.

L'article L. 931-7 du code de la sécurité sociale, dont la rédaction est identique aux articles L. 354-1 du code des assurances et L. 211-12 du code de la mutualité, dispose que les entreprises d'assurance et de réassurance mettent en place un « *système de gouvernance garantissant une gestion saine et prudente de leur activité et faisant l'objet d'un réexamen interne régulier* », **comprenant quatre fonctions** de gestion des risques, de vérification de la conformité, d'audit et actuarielle introduites par la directive « Solvabilité II ». Cet article précise que les entreprises **élaborent des politiques écrites relatives à la gestion des risques, au contrôle interne, à l'audit interne et, si besoin, à l'externalisation.**

B. LE RÈGLEMENT DIT « DORA » ET LA DIRECTIVE EPONYME INTRODUISENT DE NOUVELLES OBLIGATIONS POUR LES UNIONS ET MUTUELLES DU CODE DE LA MUTUALITÉ EN MATIÈRE DE GOUVERNANCE

La directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022, dite « DORA »[3], **intègre dans la directive « Solvabilité II » les nouvelles exigences introduites par le règlement (UE) 2022/2554** du

---

[1] *Ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.*

[2] *Rapport au Président de la République relatif à l'ordonnance n° 2015-378 du 2 avril 2015 transposant la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II).*

[3] *Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier.*

Parlement européen et du Conseil du 14 décembre 2022, dit règlement « DORA »[1], et applicables aux unions et mutuelles du code de la mutualité.

L'article 2 de la directive « DORA » vient ainsi modifier l'article 41 paragraphe 4 de la directive « Solvabilité II », **relatif aux obligations de gouvernance et de gestion des risques**, pour indiquer que les organismes d'assurance et de réassurance « *utilisent des systèmes, des ressources et des procédures appropriés et proportionnés et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil* »[2]. Le second pilier de la directive « Solvabilité II » **se voit donc complété d'un volet relatif à la gestion des risques relatifs aux technologies de l'information et de la communication**[3].

En droit interne, la prise en compte de ces évolutions du cadre européen **implique une mise à jour des dispositions du code de la sécurité sociale** et, plus spécifiquement, de son article L. 931-7 qui rassemble les dispositions relatives au système de gouvernance des institutions de prévoyance et unions régies par ce même code.

II. LE DISPOSITIF PROPOSÉ : UNE MODIFICATION DU CODE DE LA SÉCURITÉ SOCIALE VISANT À PRENDRE EN COMPTE LES NOUVELLES OBLIGATIONS ISSUES DE LA DIRECTIVE DITE « DORA » APPLICABLES AUX INSTITUTIONS DE PRÉVOYANCE ET UNIONS DE CE CODE

Le présent article complète la seconde phrase du quatrième alinéa de l'article L. 931-7 du code de la sécurité sociale pour indiquer que les institutions de prévoyance et unions du même code **mettent en place et gèrent des réseaux et des systèmes d'information conformément aux exigences du règlement « DORA ».** Cette rédaction reprend celle retenue par le premier paragraphe de l'article 2 de la directive « DORA » pour modifier le paragraphe 4 de l'article 41 de la directive « Solvabilité II », dont l'article L. 931-7 du code de la sécurité sociale assure la transposition en droit interne pour ces organismes.

---

[1] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

[2] *Article 2 de la directive « DORA ».*

[3] *Pour des développements sur le contenu des exigences introduites par le règlement « DORA », se référer au commentaire de l'article 57 du présent projet de loi.*

III. LA POSITION DE LA COMMISSION SPÉCIALE : UNE ADAPTATION NÉCESSAIRE DU CODE DE LA SÉCURITÉ SOCIALE

De manière similaire aux dispositifs portés par les articles 57 et 58 du présent projet de loi, s'agissant du code des assurances, et l'article 59 pour le code de la mutualité, le présent article prévoit une adaptation du code de la sécurité sociale pour tirer les conséquences de la modification du régime « Solvabilité II » par la directive « DORA ». Le choix du Gouvernement de reproduire la rédaction retenue par la directive permet d'assurer une transposition *a minima*.

Décision de la commission : la commission a adopté cet article sans modification.

CHAPITRE V
DISPOSITIONS FINALES

Article 62 A

Absence de double assujettissement à « DORA » et « NIS 2 »

Le présent article prévoit d'empêcher l'assujettissement à la directive « NIS 2 » des entreprises déjà assujetties aux dispositions des règlement et directive « DORA ».

La commission a adopté cet article.

I. LE DROIT EXISTANT : L'ARTICLE 4 DE LA DIRECTIVE « NIS 2 » PRÉVOIT UNE ABSENCE DE DOUBLE ASSUJETTISSEMENT ENTRE ELLE ET LES ACTES JURIDIQUES SECTORIELS SUSCEPTIBLES D'IMPOSER DES MESURES ET DES NOTIFICATIONS ÉQUIVALENTES

L'article 4 de la directive (UE) 2022/2555, dite « NIS 2 », prévoit que, lorsque des actes juridiques sectoriels de l'Union imposent à des entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents importants, et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris celles relatives à la supervision et à l'exécution, ne sont pas applicables auxdites entités. Lorsque des actes juridiques sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente directive, les dispositions pertinentes de la présente directive continuent de s'appliquer aux entités non couvertes par ces actes juridiques sectoriels de l'Union.

Certaines professions encadrées par le règlement (UE) 2022/2554 du 14 décembre 2022, dit « DORA », ont toutefois fait part au rapporteur de leur inquiétude d'être également soumis aux exigences prévues par la directive NIS 2. Ainsi, France Assureurs a fait observer que la rédaction actuelle du projet de loi n'exclut pas explicitement les assureurs du statut d'entité essentielle dans le cadre de la transposition de la directive NIS 2[1]. De même, la commission supérieure du numérique et des postes, dans l'avis qu'elle a rendu sur le sujet[2], a estimé nécessaire de préciser le régime applicable au

[1] *Réponses de France Assureurs au questionnaire du rapporteur.*
[2] *Rapport n° 2024-07 du 3 octobre 2024. Les enjeux de la transposition de la directive NIS 2 en France.*

secteur des assurances en application de la *lex specialis* pour lever les risques de double régulation entre la directive NIS 2 et le règlement DORA.

Si l'article 13 prévoit déjà que les dispositions pertinentes de la présente loi, y compris celles relatives à la supervision, ne sont pas applicables aux entités essentielles et importantes qui sont soumises, en application d'un acte juridique de l'Union européenne, à des exigences sectorielles de sécurité et de notification d'incidents ayant un effet au moins équivalent aux obligations résultant des articles 14 et 17, le rapporteur Michel Canévet estime qu'une précision plus complète peut être utile, s'agissant de l'assujettissement au règlement DORA et à la directive NIS 2.

II. LE DISPOSITIF PROPOSÉ : ÉVITER LE RISQUE DE DOUBLE ASSUJETTISSEMENT ENTRE « DORA » ET « NIS 2 »

Le présent article, résultant d'un amendement COM-132 déposé par le rapporteur Michel Canévet et adopté par la commission spéciale, prévoit que les entités financières essentielles et importantes auxquelles s'applique le titre III de la présente loi et auxquelles s'impose, en application du règlement et de la directive « DORA », l'adoption de mesures de gestion des risques en matière de cybersécurité ou la notification d'incidents importants, ne sont pas tenues de se conformer aux exigences prévues par la directive « NIS 2 », y compris celles relatives à la supervision, dès lors que l'adoption de ces mesures et la notification de ces incidents ont un effet au moins équivalent à ces exigences.

Il s'agit d'une précision utile pour éviter des mesures et notifications redondantes.

Décision de la commission : la commission a adopté cet article additionnel.

Article 62

Dates d'application des dispositions du titre III sur la résilience opérationnelle numérique du secteur financier

Le présent article prévoit une entrée en application de l'ensemble des articles du titre III à compter du 17 janvier 2025, date limite de transposition de la directive « DORA » et date d'entrée en application du règlement du même nom.

Il repousse toutefois au 17 janvier 2026 l'entrée en application des articles 46, 47 et 54 pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement « CRR », c'est-à-dire considérées comme petites et non complexes.

La date initiale du 17 janvier 2025 ne pouvant pas être tenue, la commission a adopté un amendement COM-133 du rapporteur Michel Canévet visant à prévoir l'entrée en application des articles du titre III au lendemain de la promulgation du présent texte.

Par ailleurs, bien que l'application des dispositions du paquet « DORA » aux sociétés de financement s'explique par le choix légitime fait par le passé de les soumettre aux mêmes exigences prudentielles que les établissements de crédit, elle constitue une surtransposition dont les effets ont été modérés par ce même amendement, prévoyant un report supplémentaire de l'entrée en vigueur des articles 46, 47 et 54 pour l'ensemble des sociétés de financement.

La commission a adopté cet article ainsi modifié.

I. LE DROIT EXISTANT : LE RÈGLEMENT « DORA » EST ENTRÉ EN VIGUEUR LE 17 JANVIER 2025, ÉCHÉANCE ÉGALEMENT PRÉVUE POUR LA TRANSPOSITION DE LA DIRECTIVE « DORA »

L'article 64 du règlement « DORA » prévoit que ce dernier s'applique à partir du 17 janvier 2025.

En conséquence, l'article 9 de la directive « DORA », en son premier paragraphe, prévoit que les États membres adoptent et publient les dispositions nécessaires pour s'y conformer au plus tard le 17 janvier 2025.

On rappelle ici que la directive « DORA » vient pour l'essentiel modifier les directives encadrant les secteurs bancaire et financier, dont la directive « CRD », liée au règlement « CRR », et portant sur les exigences prudentielles applicables aux établissements de crédit.

Il est précisé que le règlement « CRR » du 26 juin 2013, dans sa rédaction issue du règlement « CRR 2 » du 20 mai 2019, a introduit la notion d'« établissement de petite taille et non complexe », défini par plusieurs

critères au point 145 du paragraphe 1 de l'article 4[1]. Pour cette catégorie d'établissement, le règlement prévoit, en vertu du principe de proportionnalité, un régime simplifié de déclaration et de publication, mais aussi de calcul des ratios prudentiels (en particulier le « ratio de financement stable net », ou NSFR).

Ce régime simplifié s'applique également aux sociétés de financement qui respecte les critères prévus pour la détermination de ce qu'est un établissement de petite taille et non complexe. En France, ces sociétés sont en effet soumises aux dispositions du règlement « CRR » en vertu de l'article 2 de l'arrêté du 23 décembre 2013 relatif au régime prudentiel des sociétés de financement. Les articles L. 511-41 et suivants du code monétaire et financier prévoient également l'application du même régime prudentiel à ces sociétés et aux établissements de crédit.

II. LE DISPOSITIF PROPOSÉ : UNE ENTRÉE EN APPLICATION DU TITRE III AU 17 JANVIER 2025, À L'EXCEPTION DES ARTICLES 46, 47 ET 54 POUR LES SOCIÉTÉS DE FINANCEMENT DE PETITE TAILLE ET NON COMPLEXES

Le présent article prévoit une entrée en application de l'ensemble des articles du titre III à compter du 17 janvier 2025, date limite de transposition de la directive « DORA » et date d'entrée en application du règlement du même nom.

Il repousse toutefois au 17 janvier 2026 l'entrée en application des articles 46, 47 et 54 pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement « CRR », c'est-à-dire considérées comme de petite taille et non complexes.

III. LA POSITION DE LA COMMISSION : UN NÉCESSAIRE REPORT DE L'ENTRÉE EN VIGUEUR, Y COMPRIS POUR LES SOCIÉTÉS DE FINANCEMENT

L'examen de ce texte par le Sénat, présenté en conseil des ministres le 15 octobre 2024, était initialement prévu pour le mois de juillet 2024 mais il a été singulière retardé par la dissolution décidée par le Président de la République le 9 juin 2024 et ses suites politiques (formation du gouvernement de Michel Barnier le 21 septembre après sa nomination en tant que Premier

[1] *Il est de faible taille, la valeur de ses actifs limitée, ses obligations en matière de redressement et de résolution sont inexistantes ou simplifiées, son portefeuille de négociation est de faible taille, la valeur de ses positions sur instruments dérivés est limitée, ses actifs ou passifs consolidés liées à des activités situées en Europe sont majoritaires, il n'utilise pas de modèle interne pour satisfaire à ses exigences prudentielles, il n'a pas manifesté son opposition à être ainsi classé, de même que son autorité de supervision.*

ministre le 5 septembre, censure de celui-ci le 4 décembre, formation du gouvernement de François Bayrou le 23 décembre après sa nomination en tant que Premier ministre le 13 décembre, retard de l'examen du budget…).

Ainsi, l'avis du Conseil d'Etat sur le projet de loi, rendu public le 16 octobre, date du 6 juin 2024. Le Conseil d'Etat, dans cet avis, indique avoir été saisi du projet de loi le 7 mai 2024.

À l'époque, la perspective d'une entrée en application au 17 janvier 2025, parallèle à celle du règlement « DORA », était réaliste. Son examen retardé la rend impossible. Il est donc nécessaire d'envisager une entrée en application au lendemain de la promulgation de la loi.

Par ailleurs, l'application du paquet « DORA » aux sociétés de financement, prévue par les articles 46, 47 et 54 du titre III, constitue une surtransposition dans la mesure où elle n'est pas exigée par le droit européen.

Il pouvait donc être envisagé d'exclure ces sociétés de l'application du paquet « DORA ».

L'application de « DORA » aux sociétés de financement se justifie toutefois par le fait que les exigences prudentielles applicables aux établissements de crédit, et prévues par le règlement « CRR » et la directive « CRD », s'appliquent également aux sociétés de financement. Elles bénéficient ainsi d'un traitement prudentiel plus favorable : comme le rappelle l'étude d'impact, les expositions sur les sociétés de financement peuvent être traitées comme des expositions sur les établissements de crédit, ce qui signifie que le risque associé aux engagements auprès de sociétés de financement est réputé de même niveau qu'un établissement, évitant ainsi de décourager ces engagements.

Si, donc, l'application du paquet « DORA » aux sociétés de financement, y compris celles qui sont considérées comme de petite taille et non complexe, fait sens, une entrée en vigueur au 17 janvier 2026 pour l'ensemble de ces sociétés est de nature à instituer une différence de traitement entre les acteurs du financement spécialisé en Europe. L'Association française des sociétés financières a ainsi attiré l'attention du rapporteur sur le fait qu'en Allemagne, un arrêté du 27 décembre 2024 prévoit que les entités exerçant une activité de *leasing* seront soumises au cadre simplifié prévu à l'article 16 du règlement « DORA »[1] à partir du 1er janvier 2027. De même en Italie, l'assujettissement des entités similaires aux sociétés de financement exerçant des activités de *leasing* et de *factoring* ne devrait pas non plus intervenir avant 2027[2].

En conséquence, la commission a adopté un amendement COM-133 du rapporteur Michel Canévet visant, d'une part, à reporter l'entrée en

[1] *Les sociétés de financement françaises, soumises aux mêmes exigences prudentielles que les établissements de crédit, ne paraissent pas pouvoir relever de cet article.*

[2] *Réponses de l'Association française des sociétés financières au questionnaire du rapporteur.*

application des dispositions du titre III au lendemain de la promulgation du présent projet de loi et, d'autre part, à reporter l'application à l'ensemble des sociétés de financement des articles 46, 47 et 57 au 1er janvier 2030.

Décision de la commission : la commission a adopté cet article ainsi modifié.

TRAVAUX EN COMMISSION

I. COMPTES RENDUS DES TRAVAUX ET AUDITIONS

MARDI 12 NOVEMBRE 2024

Réunion constitutive

M. Hugues Saury, président. – Mes chers collègues, il me revient, en qualité de président d'âge, d'ouvrir la première réunion de la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Pour mémoire, un groupe de travail préfiguratif avait été constitué au mois de juin dernier afin de débuter des travaux préparatoires, avant l'adoption du projet de loi en conseil des ministres qui devait intervenir début juillet. Entre-temps, la dissolution de l'Assemblée nationale puis la constitution du nouveau gouvernement ont retardé le processus. Le projet de loi a finalement été déposé sur le bureau du Sénat en première lecture le 15 octobre.

Selon l'usage, le bureau de la commission spéciale est constitué, à la proportionnelle des groupes, d'un président, de dix vice-présidents et de trois secrétaires.

Pour les fonctions de président, j'ai reçu la candidature de M. Olivier Cadic, du groupe Union Centriste.

La commission spéciale procède à la désignation de son président, M. Olivier Cadic.

M. Olivier Cadic, président. – Mes chers collègues, je vous remercie de m'avoir confié la présidence de cette commission spéciale.

Alertés sur l'urgence à transposer certaines directives européennes avant le 17 octobre de cette année, nous avions constitué un groupe de travail préfiguratif avant l'été.

Cette date est déjà dépassée, mais le calendrier qui nous attend n'en est pas moins contraint. L'examen en séance publique pourrait intervenir lors de la semaine gouvernementale du 10 février 2025. Dans cette hypothèse, la réunion de commission pour l'adoption du texte devrait se tenir la dernière semaine de janvier. Compte tenu de l'examen du projet de loi de finances pour 2025, puis de la suspension des travaux parlementaires, c'est demain, ou presque ! Nous devrons donc nécessairement limiter les auditions en réunions plénières. Toutefois, sans préempter le travail des rapporteurs, leurs auditions seront sans doute ouvertes à tous les membres de la commission spéciale.

Je vous propose désormais de passer à la nomination des vice-présidents et des secrétaires. La règle qui s'applique est celle des commissions permanentes. En conséquence, le nombre de vice-présidents est de dix et celui de secrétaires de trois.

La répartition par groupe politique est la suivante : pour le groupe Les Républicains, trois vice-présidents et un secrétaire ; pour le groupe Socialiste, Écologiste et Républicain, deux vice-présidents et un secrétaire ; pour le groupe Union Centriste, un secrétaire – en plus du poste de président qui m'a été confié – ; pour le groupe Rassemblement des démocrates, progressistes et indépendants, un vice-président ; pour le groupe Communiste Républicain Citoyen et Écologiste – Kanaky, un vice-président ; pour le groupe du Rassemblement Démocratique et Social européen, un vice-président ; pour le groupe Les Indépendants – République et Territoires, un vice-président ; pour le groupe Écologiste – Solidarité et Territoires, un vice-président.

Compte tenu des candidatures qui sont parvenues au secrétariat de la commission spéciale, je vous propose la désignation comme vice-présidents : pour le groupe Les Républicains, M. Cédric Perrin, Mme Christine Lavarde et M. André Reichardt ; pour le groupe Socialiste, Écologiste et Républicain, Mmes Hélène Conway-Mouret et Audrey Linkenheld ; pour le groupe Rassemblement des démocrates, progressistes et indépendants, Mme Nadège Havet ; pour le groupe Communiste Républicain Citoyen et Écologiste – Kanaky, Mme Michelle Gréaume ; pour le groupe du Rassemblement Démocratique et Social européen, M. Bernard Fialaire ; pour le groupe Les Indépendants – République et Territoires, Mme Vanina Paoli-Gagin, pour le groupe Écologiste – Solidarité et Territoires, M. Akli Mellouli.

Les vice-présidents sont désignés.

M. Olivier Cadic, président. – Je vous propose, conformément aux propositions formulées par les groupes, la désignation comme secrétaires : pour le groupe Les Républicains, M. Étienne Blanc ; pour le groupe Socialiste, Écologiste et Républicain, M. Rémi Cardon ; pour le groupe Union Centriste, Mme Catherine Morin-Desailly.

Les secrétaires sont désignés.

M. Olivier Cadic, président. – Aux fonctions de rapporteurs, j'ai reçu les candidatures de M. Patrick Chaize et M. Hugues Saury pour le groupe Les Républicains, de M. Michel Canévet pour le groupe Union Centriste.

M. Hugues Saury, M. Patrick Chaize et M. Michel Canévet sont désignés rapporteurs.

M. Olivier Cadic, président. – Nous tiendrons très rapidement une réunion de bureau pour décider de l'organisation de nos travaux.

Je souhaite notamment que nous puissions entendre rapidement Mme Clara Chappaz, secrétaire d'État auprès du ministre de l'enseignement

supérieur et de la recherche, chargée de l'intelligence artificielle et du numérique, avec qui j'ai eu un entretien téléphonique la semaine dernière. Je vous proposerai ensuite quelques auditions de services concernés, comme notamment l'Agence nationale de la sécurité des systèmes d'information (Anssi), et quelques tables rondes.

Je souhaiterais également que nous puissions nous rendre à Bruxelles pour entendre la nouvelle Commission européenne. J'ai par ailleurs appris que la Belgique avait d'ores et déjà procédé à la transposition de la directive du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite NIS2 : nous pourrons donc également échanger avec nos homologues belges et le gouvernement fédéral sur leur vision de la cybersécurité.

Enfin, je voudrais signaler plusieurs caractéristiques du texte qui nous occupe.

En premier lieu, celui-ci est passé de 47 articles, dans la version préparatoire qui nous avait été communiquée avant l'été, à 62 articles dans sa version actuelle. Je m'en suis étonné lors de ma conversation avec la secrétaire d'État. Selon elle, il s'agirait de précisions légistiques apportées à la suite de l'avis du Conseil d'État. Il nous faudra toutefois être vigilants pour éviter toute surtransposition et l'insertion de dispositions qui ne relèveraient pas de la transposition des directives, car ce texte pourrait alors s'apparenter à un « Ddadue », c'est-à-dire un texte portant « diverses dispositions d'adaptation au droit de l'Union européenne ».

En second lieu, ce projet de loi vise la transposition de trois directives distinctes : outre la directive NIS 2, la directive du 14 décembre 2022 sur la résilience des entités critiques, dite REC, qui vise à modifier le code de la défense, et la directive du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, dite Dora, cette dernière relevant davantage du domaine de la commission des finances.

Chacun de ces textes se voit consacrer un titre spécifique dans le projet de loi, ce qui assure la lisibilité du partage des compétences entre nos trois rapporteurs, sous réserve d'une répartition plus fine de certaines dispositions du titre II ayant trait à l'Anssi.

M. Hugues Saury, rapporteur. – En tant que rapporteur de la commission des affaires étrangères, de la défense et des forces armées, il me reviendra d'instruire le titre I^er^ du projet de loi, qui transpose en droit français la directive REC, ainsi que certaines dispositions du titre II concernant l'Anssi.

S'agissant de la transposition, le Gouvernement a fait le choix de ne pas repartir d'une page blanche, mais de procéder à une réécriture du dispositif actuel de sécurité des activités d'importance vitale créé en 2006, qui figure dans le code de la défense et qui est désormais connu et maîtrisé par les opérateurs concernés.

Le projet de loi définit le régime de désignation des « opérateurs d'importance vitale » (OIV).

Il reprend la logique actuelle de protection des opérateurs à leurs frais reposant sur une obligation de résultat, et non de moyens. Les opérateurs détermineront donc eux-mêmes les moyens mis en œuvre dans des documents renommés « plans de résilience », l'idée étant de passer d'une logique de protection à une logique de résilience.

Le texte vise à mieux prendre en compte et identifier les interdépendances des opérateurs et des vulnérabilités éventuelles de leurs chaînes d'approvisionnement.

Il prévoit également de généraliser le régime de notification des incidents à l'autorité administrative, qui ne concerne à l'heure actuelle que quelques secteurs.

Il définit aussi des entités critiques d'importance européenne, fournissant des services essentiels dans au moins six États membres.

Enfin, il met en place une « commission des sanctions », avec le passage d'un régime de sanctions pénales à un régime de sanctions administratives, diverses dispositions étant par ailleurs prévues afin de garantir l'indépendance de cette commission.

S'agissant d'une transposition d'un texte européen, nos marges de manœuvre seront sans doute assez minces, d'autant qu'il est dans l'intérêt des opérateurs concernés que les règles soient, dans une large mesure, homogènes sur l'ensemble du territoire de l'Union européenne.

Comme mes collègues rapporteurs, je m'attacherai en particulier à contrôler que les dispositions figurant dans le projet de loi ne vont pas au-delà de ce qui existe actuellement ou de ce qui est strictement requis par la directive.

M. Patrick Chaize, rapporteur. – C'est dans un contexte nouveau, présentant une configuration politique renouvelée, que nous devons mener à bien l'examen de ce projet de loi, initialement prévu en juillet dernier…

Le texte découle directement du droit de l'Union européenne et des initiatives prises par la Commission européenne pour renforcer et harmoniser les règles de cybersécurité applicables aux entités critiques et aux entreprises stratégiques du marché intérieur. Vous l'aurez compris, c'est, une nouvelle fois, un projet de loi « Ddadue » qui ne dit pas son nom !

Rapportant au nom de la commission des affaires économiques, je serai notamment chargé d'examiner le titre II, traitant de la transposition de la directive NIS 2.

Cette directive devait être transposée au plus tard le 17 octobre 2024, mais, je vous rassure, nous ne sommes pas les seuls en retard. Pour l'heure,

seuls deux États membres l'ont pleinement transposée en droit interne : la Belgique et l'Italie.

Cette directive est très importante, car elle témoigne d'un changement de paradigme et d'une plus grande prise de conscience des risques pesant sur nos entreprises et nos infrastructures. Alors que la précédente directive NIS 1, qui, datant de 2016, a désormais été abrogée, s'appliquait à 500 opérateurs d'importance vitale et à six secteurs d'activités, la directive NIS 2 s'applique à des milliers d'entités et à dix-huit secteurs d'activité, permettant une mobilisation générale du monde économique.

C'est pourquoi l'Anssi et le secrétariat général de la défense et de la sécurité nationale (SGDSN) ont élaboré ce projet de loi, après plusieurs phases de consultation menées auprès de soixante-dix-neuf fédérations professionnelles et treize associations d'élus, ce que nous pouvons saluer.

Sont par exemple concernées les entreprises de production, de distribution et de gestion des réseaux d'énergie, les infrastructures numériques, les entreprises de transport, les administrations et les collectivités territoriales – le Gouvernement a fait le choix judicieux de les intégrer au périmètre d'application de cette directive.

Dans une moindre mesure, les organismes de recherche, les entreprises de télécommunications, de services postaux, de gestion des déchets, de denrées alimentaires, de produits chimiques, de production automobile ou encore de produits informatiques sont également concernés.

Face à l'ampleur du champ d'application concerné, je serai particulièrement vigilant à la fixation des délais de mise en œuvre, à l'application des sanctions, à l'identification des responsabilités et à l'élaboration de dispositifs d'accompagnement des entreprises afin de mettre en œuvre, dans un souci de pragmatisme, la transition nécessaire vers l'application de cette nouvelle réglementation.

M. Michel Canévet, rapporteur. – En qualité de rapporteur de la commission des finances, je serai en charge du titre III du projet de loi, dont l'objet est de transposer la directive Dora.

La gestion des risques informatiques et la protection contre les cyberattaques ont été quasiment absentes des modifications de la réglementation européenne du secteur financier adoptées après la crise financière de 2008. Les États membres ont dès lors mis en place leurs propres réglementations nationales, conduisant à une fragmentation des obligations, alors que le degré élevé d'interconnexion des services financiers rend nécessaire la mise en place d'un cadre commun au niveau de l'Union européenne. C'est la raison pour laquelle a été adopté, en décembre 2022, un règlement sur la résilience opérationnelle du secteur financier, accompagné d'une directive.

Le règlement Dora, applicable à partir du 17 janvier 2025, vise deux objectifs principaux : d'une part, harmoniser le cadre de prévention, de détection et de *reporting* des incidents numériques, applicable à toutes les entités financières dans l'Union européenne ; d'autre part, créer des règles communes encadrant le recours à des prestataires de services par les entités financières.

La directive Dora est, quant à elle, essentiellement d'ordre technique et vise à insérer des renvois au règlement Dora au sein du corpus législatif européen existant.

Les articles du titre III du projet de loi comportent pour l'essentiel des mesures de coordination prévues par la directive Dora, notamment pour actualiser les références dans plusieurs codes – code monétaire et financier, code de la mutualité, code des assurances et code de la sécurité sociale.

L'existence d'un règlement Dora, d'application directe, et la nature essentiellement technique de la directive Dora limitent nos marges de manœuvre. Néanmoins, vous le savez, sous couvert de dispositions de coordination, certaines surprises peuvent apparaître… Nous devrons donc veiller à ce que la transposition de la directive Dora n'introduise pas d'obligations qui iraient au-delà de ce qui est requis par le droit européen.

M. Olivier Cadic, président. – Les Suisses ont remporté les Mondiaux des métiers de la cybersécurité. Je me suis renseigné sur le cycle de formation qu'ils mettaient en œuvre pour atteindre ce niveau : il s'agit, en fait, d'une collaboration entre l'industrie de la finance, qui, comme vous le savez, est très puissante dans ce pays, et l'armée. Ensemble, ils forment les ingénieurs travaillant dans le secteur de la finance, ceux-ci étant mis à disposition de la défense en cas de besoin.

Mme Catherine Morin-Desailly. – Serait-il possible, au démarrage de nos travaux, d'appréhender la question de la cybersécurité de manière systémique, au regard notamment des textes européens déjà votés ?

Je pense au règlement sur les services numériques (DSA ou *Digital Services Act*), au règlement sur les marchés numériques (DMA ou *Digital Markets Act*), au règlement sur l'intelligence artificielle (*IA Act*), au règlement sur les données (*Data Act*), mais également au règlement établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir.

Lors de nos travaux sur la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN), visant à adapter les différents textes que je viens de mentionner, nous avions pris certaines dispositions pour donner aux organismes d'importance vitale les moyens de leur cybersécurité.

Il me semble important d'appréhender de manière globale l'état des menaces et les réponses qui sont apportées.

Par ailleurs, au-delà de l'Anssi, ne faudrait-il pas auditionner la Commission nationale de l'informatique et des libertés (Cnil), qui est concernée par les questions portant sur l'intelligence artificielle et qui pourrait se voir attribuer le rôle d'autorité chargée de l'application du texte ?

M. Olivier Cadic, président. – J'ai demandé de disposer d'un bilan de l'application de la directive NIS1, ce qui répond partiellement à votre questionnement. Par ailleurs, des dispositions votées dans la loi SREN ne sont toujours pas appliquées, comme le filtre anti-arnaque. Enfin, pour plusieurs sujets, on est en droit de se demander s'il faut passer par la loi ou pas.

Comme je l'ai indiqué, je vous propose en premier lieu d'entendre la secrétaire d'État, puis de rencontrer les représentants de la Commission européenne pour voir si la transposition envisagée par le gouvernement français correspond à leur attente – n'oublions pas que l'on cherche à hausser le niveau de sécurité dans toute l'Union européenne. Votre proposition d'entendre la Cnil me semble tout à fait judicieuse, ne serait-ce qu'au sujet des sanctions ; je la retiens donc. Les rapporteurs, de leur côté, feront aussi des suggestions.

Mme Anne-Catherine Loisier. – Pourrions-nous disposer d'une note qui reprendrait tous les points stratégiques liés à la transposition des directives ?

M. Olivier Cadic, président. – Effectivement, il serait naturel d'avoir un cadrage de départ, notamment sur l'objectif de NIS 2 par rapport à NIS 1, pour nous mettre tous au même niveau d'information.

M. Thomas Dossus. – Avez-vous des éléments de calendrier à nous communiquer ?

M. Olivier Cadic, président. – Le calendrier sera arrêté lors de la réunion de bureau. Je souhaite que les professionnels puissent intervenir sous forme de table ronde, car vous risquez d'être très sollicités.

Mme Anne-Catherine Loisier. – Je me rappelle d'un entretien à ce sujet avec des opérateurs de territoires ultramarins. Ce serait bien de ne pas oublier cette dimension de la question.

M. Olivier Cadic, président. – Ce pourrait être dans le cadre d'une audition que j'aimerais organiser, avec possibilité d'interventions à distance. Nous y gagnerions.

MARDI 17 DÉCEMBRE 2024

1. Entreprises et cybersécurité – Audition des représentants du Mouvement des entreprises de France (Medef) et de la Confédération des PME (CPME)

M. Olivier Cadic, président. – C'est avec un grand plaisir que j'ouvre aujourd'hui le cycle des auditions qui seront consacrées au projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Je rappelle que notre commission spéciale s'est constituée le 12 novembre dernier pour examiner ce texte qui vise à transposer trois directives différentes : celle portant sur la résilience des entités critiques, dite directive REC ; celle concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite directive NIS 2 ; enfin, celle concernant la résilience opérationnelle numérique du secteur financier, dite directive Dora.

Cette transposition devait intervenir avant le 17 octobre ; toutefois, le contexte politique actuel explique le retard de nombreux projets de loi. Cela dit, les entreprises attendent avec impatience de connaître les nouveaux objectifs de cybersécurité et les nouvelles obligations qui leur incomberont.

C'est pourquoi je remercie le Mouvement des entreprises de France (Medef) et la Confédération des petites et moyennes entreprises (CPME) d'avoir répondu à notre invitation pour partager leur point de vue sur le projet de loi et sur l'impact de cette transposition ainsi que, le cas échéant, vos propositions. Nous pourrons ainsi relayer vos préoccupations auprès du directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), que nous auditionnerons après vous. L'Union des entreprises de proximité (U2P) et l'Association française des entreprises privées (Afep) m'ont fait savoir que leur position n'était pas encore arrêtée et qu'elles nous adresseraient ultérieurement leur contribution écrite.

Pour le Medef, nous accueillons : Mme Maxence Demerlé, directrice du numérique ; M. Maxime Foret, chargé de mission sénior au sein du pôle Affaires publiques ; et Mme Mathilde Briard, chargée de mission Économie numérique.

La CPME est représentée par : Mme France Charruyer, membre de la commission numérique ; M. Lionel Vignaud, directeur des affaires économiques, juridiques et fiscales ; M. Jérôme Normand, économiste ; et M. Adrien Dufour, responsable des affaires publiques.

Avant de vous céder la parole, je rappelle que cette audition fait l'objet d'une captation vidéo qui est retransmise sur le site internet du Sénat puis consultable en vidéo à la demande.

Pour ouvrir cette table ronde, je propose que vous présentiez vos positions sur le texte puis je donnerai la parole à chacun des rapporteurs, MM. Michel Canévet, Patrick Chaize et Hugues Saury, puis à ceux de nos collègues qui le souhaitent.

J'en profite pour vous indiquer que le « 17 cyber » a été lancé ce matin. À cette occasion, il a été rappelé plus de 60 % des entreprises ne sont pas conscientes d'être exposées aux risques numériques.

Mme Maxence Demerlé, directrice du numérique du Medef. – Nous sommes nous aussi très heureux que la plateforme cybermalveillance.gouv.fr se transforme en « 17 cyber » ; c'est un outil extrêmement pratique que le Medef attendait avec impatience.

Le Medef regroupe 101 fédérations qui rassemblent des entreprises de toutes tailles et de tous secteurs d'activité. Nous disposons de 120 représentations dans les territoires.

Nous organisons actuellement un Tour de France de l'IA (intelligence artificielle) : nous sentons que les chefs d'entreprise ont envie de comprendre les enjeux de l'économie numérique. C'est l'occasion de recenser des cas d'usage, mais aussi des incidents cyber, tels que les rançongiciels. Ces cybermenaces se multiplient, mais les chefs d'entreprise n'en sont pas toujours conscients. Hélas, les chiffres sont éloquents : le parquet de Paris a ainsi ouvert 512 nouvelles enquêtes pour ce type d'affaires en 2023, soit une augmentation de 22 % par rapport à l'année précédente.

Dans son rapport annuel consacré aux cybermenaces, l'Agence européenne pour la cybersécurité (Enisa) signale que l'un des plus grands acteurs du rançongiciel, LockBit 3.0, a fait de la France sa deuxième cible mondiale après les États-Unis. Notre pays est sur le podium des nations les plus menacées : le numérique, c'est aussi politique, et pas seulement technologique. C'est pourquoi nous sommes très heureux d'évoquer les moyens visant à renforcer notre cyber-résilience devant la représentation nationale.

Nous accueillons ce texte dans un esprit positif et constructif. Le Medef s'était beaucoup impliqué dans la transposition de la directive NIS 1 . Moins de dix ans plus tard, nous examinons la deuxième version de cette directive, qui élargit considérablement le nombre de secteurs et d'entreprises concernés.

Persuader les entreprises de s'intéresser à la cybersécurité représente un Everest à gravir, compte tenu du nouveau périmètre prévu par le texte, dont les contours sont imprécis. La définition des entités importantes et des entités essentielles devrait être précisée. De nombreuses entreprises nous ont contactés pour savoir si elles étaient ou non concernées.

Aux termes de l'article 8, les entités essentielles sont définies comme des entreprises employant au moins 250 personnes ou dont le chiffre d'affaires

annuel excède 50 millions d'euros annuels. Nous souhaitons que ce critère soit non pas alternatif, mais cumulatif. Il en va de même pour les entités importantes, définies à l'article 9. Cette recommandation nous semble d'autant plus importante que l'article 12 prévoit que l'Anssi établisse la liste de ces entités sur la base de leurs déclarations.

Certaines entreprises nous ont fait part de leurs doutes sur leur classification comme entité essentielle ou entité importante. Là encore, une clarification s'impose. Peut-être l'Anssi pourrait-elle les aider à déterminer si elles sont concernées par l'application de la directive.

Nous nous réjouissons que le caractère proportionnel des dispositions applicables aux entités essentielles et entités importantes soit bien prévu par le projet de loi ; nous y sommes très attachés.

Nous souhaiterions que la même philosophie s'applique aux mesures qui seront exigées des entreprises par l'Anssi. Les entités importantes sont définies à l'article 9 comme des entreprises employant au moins 50 personnes ou dont le chiffre d'affaires excède 10 millions d'euros. Avec une telle définition, de nombreuses entreprises de taille moyenne seraient concernées. Or celles-ci ne disposent souvent pas du budget suffisant pour mettre en place des mesures ambitieuses : souvent, elles n'ont pas à proprement parler de directeur des services informatiques (DSI) ; quand elles ont en un, le poste est parfois externalisé. Les recommandations de l'Anssi devront donc être adaptées à la réalité de ces structures.

L'article 10 du projet de loi prévoit que le Premier ministre peut désigner par arrêté comme entité essentielle ou comme entité importante une entité exerçant une activité relevant d'un secteur d'activité hautement critique ou critique, quelle que soit sa taille, sous réserve de justifier cette désignation par le respect de certains critères. Un recours contre cette décision sera-t-il possible ? Nous souhaiterions introduire un échange contradictoire.

De combien de temps les entreprises disposeront-elles pour se mettre en conformité avec ces nouvelles dispositions ? Le texte est muet sur ce point. Nous aimerions que des précisions à ce sujet y soient intégrées, ou, à tout le moins, évoquées lors des débats parlementaires. Nous préconisons un délai de trois ans, à l'image de ce que prévoyait la directive NIS 1, car les entreprises ont besoin de définir précisément les objectifs et les formations nécessaires pour se mettre en conformité avec les nouvelles règles, et donc prévoir les fonds en conséquence. Les sommes que consacrent les entreprises de moins de 10 salariés à l'informatique, matériel inclus, s'élèvent entre 2 000 et 3 000 euros par an. Or le précédent directeur général de l'Anssi estimait que 10 % à 15 % du budget total consacré à l'informatique devait porter sur des dépenses liées à la cybersécurité. Cela représente des sommes peu élevées pour les petites entreprises. Nous avons donc besoin de temps pour clarifier et planifier les choses.

Nous souhaiterions mieux comprendre les dispositions de l'article 11. Comment s'applique la directive pour les groupes ? Nombre de nos adhérents ont des activités dans plusieurs pays. Or l'article évoque notamment les entreprises établies sur le territoire national. Mais cette notion n'est pas évidente : le siège du groupe n'est pas nécessairement en France. En outre, *quid* des filiales ?

Le III de l'article 11 dispose que l'établissement principal s'entend du lieu où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Mais le I ne contient nulle référence à cette notion d'établissement principal.

Nous avons donc besoin de clarifications : les dispositions du texte s'appliqueront-elles parce que l'établissement principal est situé en France ou parce que l'établissement dépasse le seuil de salariés ou de chiffre d'affaires ? Par extension, les filiales de l'entreprise situées à l'étranger devront-elles respecter la loi française, même si elles ne dépassent pas le seuil ? Plusieurs de nos adhérents ont des activités dans d'autres pays européens : ils ont besoin de comprendre la façon dont les règles s'appliqueront.

L'article 17 porte sur la notion d'incident important, un critère majeur pour le déclenchement de certaines procédures prévues par le texte. Celles-ci devrait être mieux précisées. L'incident est déterminé par un acte d'exécution qui vient d'être pris pour les entreprises de services numériques. Dans un esprit d'harmonisation, nous souhaiterions que les critères de cet acte servent de base pour définir un incident important afin de ne pas créer de distorsion d'un pays à l'autre et d'éviter le cybershopping : tous les États doivent être mis sur un pied d'égalité. Nous avons aussi un objectif sous-jacent : faire en sorte que le marché de la cybersécurité puisse être à la portée de nos entreprises. Notre pays a la chance de compter de nombreuses firmes spécialisées dans la cybersécurité : l'objectif sous-jacent est de mettre ce marché à leur portée. Nous appelons donc à une transposition harmonisée, qui crée le moins possible de nouvelles obligations.

L'article 5 désigne l'Anssi comme l'entité responsable de la mise en œuvre de ce texte. C'est elle qui sera chargée d'effectuer les contrôles prévus. L'Agence dispose de compétences techniques extraordinaires, qui ont contribué à faire de la France un pays sécurisé en matière cyber, alors que la menace pesant sur notre pays est réelle. Mais elle est placée sous l'autorité du Premier ministre et rattachée au secrétariat général de la défense et de la sécurité nationale (SGDSN) : cette position était logique lorsqu'elle assurait uniquement la cybersécurité des systèmes d'information de l'État. Est-elle toujours pertinente ? Par ailleurs, l'Anssi disposera-t-elle des moyens suffisants pour agir ? Des représentants des acteurs économiques pourraient-ils être associés à sa gouvernance, à l'instar des collèges créés par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) ou par la Commission nationale de l'informatique et des libertés (Cnil) ? Les relations entre le monde économique

et les délégués régionaux de l'Agence sont excellentes, mais ces derniers ne sont pas très nombreux. Comment accompagner au plus près les entreprises ?

Le texte n'évoque pas le rôle des centres de réponse aux incidents de sécurité informatique (CSIRT), ou *Computer security incident response team* en anglais. Ces structures créées par les conseils régionaux accomplissent un travail de bonne qualité, mais disposent de peu de moyens. En outre, l'articulation avec la plateforme Cybermalveillance est peu développée : c'est dommage, car celle-ci est pourtant un bel exemple de partenariat public-privé réussi.

Mme France Charruyer, membre de la Commission numérique de la CPME. – Je vous remercie de l'occasion unique qui nous est offerte de collaborer avec le Sénat et de présenter les actions menées par la CPME sur le terrain.

La CPME compte 243 000 adhérents, 133 structures territoriales et 122 fédérations patronales. Aujourd'hui, la question qui lui est posée est de savoir comment embarquer les dirigeants qu'elle représente dans la gestion du nouveau risque numérique.

En tant qu'entrepreneur et avocat délégué à la protection des données au service des entreprises, j'ai une approche de terrain. C'est pourquoi je tiens à présenter les dispositifs innovants mis en place au sein de la CPME. En effet, en la matière, il s'agit non pas de surtransposition ou de tout régler par la norme, mais de savoir si les dirigeants sont capables d'absorber des chocs toujours plus nombreux et de faire face à l'imprévu, alors qu'on dénombre actuellement 66 000 défaillances d'entreprises. Comment peut-on les encourager dans cette direction lorsqu'ils sont quotidiennement confrontés à un manque de trésorerie et qu'ils doivent eux-mêmes embarquer leurs salariés dans la transformation numérique ?

Cette dernière revêt des obligations légales définies par le code du travail – je le rappelle ; il n'a pas fallu attendre la directive NIS 2 pour cela. Ainsi en est-il de l'obligation générale de sécurité, dite *by-design*, résultant de l'article 32 du règlement général sur la protection des données (RGPD) et des nouvelles obligations sectorielles issues des directives NIS 2 et Dora, de la loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (Lopmi), de la loi de programmation militaire (LPM) ou encore du *Cyber Resilience Act* (CRA). Dans cet enfer réglementaire, dont les enjeux se mesurent en réalité au niveau des États, le droit est une arme de défense économique. Aussi, pour faire adhérer les dirigeants aux dispositifs prévus, il faut non pas se contenter de développer un marketing de la peur ou un marketing normatif, mais entrer dans cette chaîne de valeur.

Par conséquent, la CPME a mis en place des commissions dédiées à la sécurité économique, car il n'est pas souhaitable d'aborder la question de la cybersécurité sous le prisme de la sanction. En la matière, il faut expliquer aux dirigeants que le patrimoine informationnel de leur entreprise est un actif à

protéger. La CPME a aussi mis en œuvre de petites choses, car les entreprises qu'elle représente sont de taille modeste – des très petites entreprises (TPE) et des PME innovantes, quelques entreprises de taille intermédiaire (ETI) –, comme une convention de partenariat avec des centres de réponse aux incidents cyber territoriaux, les CSIRT, par exemple Cyber'Occ dans la région Occitanie ou le campus régional de cybersécurité et de confiance numérique de la région Nouvelle-Aquitaine qui fonctionnent très bien. Nous avons également développé des formations gratuites destinées aux dirigeants. Aussi, la première difficulté en la matière aura trait au changement d'échelle induit.

La deuxième difficulté est liée à la disponibilité de trésorerie nécessaire pour remédier à un problème de cybersécurité. En effet, la question est alors non pas de savoir si les bonnes cases d'une documentation ont été remplies, mais de disposer de trois mois de trésorerie d'avance. Malheureusement, c'est le cas de très peu d'entreprises.

La troisième difficulté est liée à la bonne compréhension de la norme. Selon l'enquête à laquelle ont participé la CPME, le Medef et la plateforme cybermalveillance.gouv.fr, moins d'une entreprise sur deux est dotée d'une solution de détection et une majorité des dirigeants sondés avouent méconnaître la norme en vigueur. Ainsi ne connaissent-ils pas le sens de l'acronyme NIS 2, encore moins celui de la Lopmi, loi qui leur permettrait de profiter de garanties assurantielles. Ils méconnaissent totalement les règles et les obligations de déclaration ou de notification. Par conséquent, ils ne peuvent pas anticiper les actions à mettre en place dans ce domaine.

La nouvelle réglementation est-elle accessible à tous et définie à la bonne échelle ? L'Anssi a indiqué qu'un délai de transition de trois ans était prévu. Nous avons besoin que soit prise en compte la courbe d'apprentissage des entreprises, comme ce fut le cas en 2018 lors de l'entrée en application du RGPD, et que cela soit inscrit.

Si le périmètre nous pose le même problème qu'au Medef, nous en avons un autre plus important. Au sein du tissu économique de la CPME, l'ensemble des sous-traitants qui participent à la chaîne de valeur seront concernés, mais aussi ceux qui voudront ou devront travailler avec les grosses entreprises ; dans ce cas, le standard en vigueur écrase tout. La norme ne servira-t-elle pas de nouveau de bouclier, comme ce fut le cas pour les Gafam ? Je le rappelle : 96 % des données de nos entreprises sont hébergées par des sociétés soumises à une réglementation extraterritoriale.

C'est pourquoi il serait souhaitable de s'intéresser à la valeur de l'actif à protéger et, peut-être, aux dispositifs incitatifs en la matière plutôt qu'aux sanctions. En effet, pour embarquer les petites PME dans cette transformation, il faut d'abord leur expliquer comment se mettre en conformité avec l'état de l'art dans ce domaine et, par conséquent, faire œuvre de pédagogie. Sur le terrain, la CPME a donc conclu des conventions de partenariat avec les CSIRT financés par les régions, qui devront disposer de davantage de moyens.

En effet, les entreprises aujourd'hui ne disposent pas de solutions de détection, car celles-ci reposent en majorité sur des dispositifs très puissants faisant appel à l'intelligence artificielle (IA), comme l'*Open Source Intelligence* (Osint), qui ne sont pas à la portée des PME. Or comment les entreprises peuvent-elles savoir si elles sont victimes de fuites de données, notamment sur le *clear web,* sans accéder à ces technologies ? Des accords ont été signés avec des compagnies d'assurance qui réalisent des « scans cyber » selon une logique de prévention des risques. Mais est-ce le rôle des assureurs ou celui des entreprises ou des syndicats d'entreprises ? Non. Nous avons la chance de disposer des CSIRT, qui fonctionnent très bien et qui pourraient devenir des lanceurs d'alerte en collaboration avec l'Anssi, s'ils étaient dotés de tels outils technologiques, selon les termes de l'article 24 du projet de loi. L'Anssi et les CSIRT doivent donc disposer de moyens supplémentaires.

Un deuxième problème a trait à la lisibilité de la norme ; cette dernière doit avoir un sens et indiquer une direction. Or il existe plusieurs définitions de la notion d'incident, selon notamment le RGPD, les directives NIS 2 et Dora, ou le règlement sur la cyber-résilience. Il faut être un fin juriste pour s'y retrouver ! Pour ce qui concerne la notion de risque, ce terme figure cent soixante-dix-sept fois dans le règlement européen sur l'intelligence artificielle (RIA), mais sa définition est différente. Il serait donc nécessaire de réfléchir à un « commun numérique », à savoir une réglementation harmonisée, que nous appelons de nos vœux. Cela suppose d'arrêter la guerre que se livrent les régulateurs européens et, en France, de faire travailler ensemble les deux régulateurs que sont la Commission nationale de l'informatique et des libertés (Cnil) et l'Anssi, tout en les dotant de moyens supérieurs, afin de ne plus faire peser le risque sur les plus petits éléments de la chaîne, qui n'en peuvent plus – en témoignent les 66 000 défaillances d'entreprises. Or ce sont des maillons essentiels : sans eux, la chaîne de sous-traitance ou la logistique ne fonctionnent pas. Ils n'y arrivent pas par manque de trésorerie, parce qu'ils ne savent pas lire la norme, parce qu'ils ne sont dotés ni de direction générale, ni de délégué à la protection des données (DPO, pour *Data Protection Officer*), ni de responsable de la sécurité des systèmes d'information (RSSI) mutualisé. C'est pourquoi ils font appel à un réseau de bénévoles, dont la CPME fait partie, car la souveraineté commence par la défense de la compétitivité des territoires.

Ainsi, trois conditions doivent être réunies pour transformer les dirigeants en entrepreneurs de la donnée : il faut d'abord qu'ils prennent conscience de ce qu'ils possèdent, ensuite, qu'ils connaissent l'écosystème, enfin, que les CSIRT qui détiennent des solutions de détection des incidents et de fuites de données deviennent des lanceurs d'alerte. À cela doit s'ajouter une nécessaire proportionnalité ; l'Anssi nous soutient en la matière, car elle a conscience qu'il faudra plus de trois ans pour y parvenir. Nous avons su le faire lors de la mise en œuvre du RGPD, nous saurons aussi le faire dans le cas présent.

La norme et les standards européens ne doivent pas se retourner contre nos entreprises. Il ne s'agit pas d'entreposer notre mémoire dans les archives d'un autre. La souveraineté appartient à celui qui détient le pouvoir d'exception.

La cybersécurité est une arme d'intelligence économique. Dans ce domaine, nous avons besoin de tous les maillons de la chaîne économique. À l'heure de l'IA générative, les entreprises déploient la solution Copilot, sans en avoir réellement conscience et sans avoir les moyens de paramétrer Purview, c'est-à-dire l'étiquetage de la donnée ; elles n'ont pas les moyens de se doter de DPO, mais elles savent comment mutualiser.

Aujourd'hui, nous avons l'occasion unique de doter nos institutions et nos organes de contrôle de moyens suffisants. Ne faites pas peser sur les entreprises le poids de cette cybersurveillance, de cette cybercompétence, puisque les organisations doivent se transformer en systèmes autoapprenants. Il faut faire preuve de réalisme et de modestie, mais aussi comprendre comment les investissements dans la cybersécurité transformeront une entreprise en une société productrice de bases de données, ce qui dépassera la notion de charge et sera pris en compte dans la mesure de la performance extrafinancière des entreprises. Depuis deux ans, les fonds d'investissement demandent des *Technical Due Diligence* et s'intéressent enfin à la solidité et à la robustesse du système d'information (SI) et de l'outil informatique pour investir, car l'argent magique, c'est fini.

Pour faire entrer les chefs d'entreprise dans la chaîne de valeur de la cyber-économie, il faut libérer le patrimoine numérique des entreprises et faire confiance aux entrepreneurs. Les textes qui comprennent uniquement des sanctions seront contre-productifs, parce que lisibles uniquement par les plus gros entrepreneurs. Une forme de cannibalisme se mettra alors en place, ce qui posera des questions de fermeture du marché. On se retrouvera avec une cybersécurité *made in* Microsoft, avec des outils d'IA génératives qui sont en réalité des éponges à données et à secrets d'affaires. L'Anssi a réalisé un travail remarquable avec les CSIRT pour remettre la réglementation à l'endroit.

Nous souhaitons donc aussi de la proportionnalité et une meilleure définition du périmètre ; nous savons que nous l'obtiendrons. En réalité, il est question de moyens. Aussi, ne nous refilez pas la patate chaude, si je puis dire.

Un syndicat professionnel signe une convention avec des CSIRT – le Medef et les chambres de commerce et d'industrie (CCI) en ont également signé une –, pour mettre en place cette cybersécurité. Selon un CSIRT, la moyenne générale des scores d'une PME s'élève à 1,4 sur 5 ; nous devrons donc gravir cette échelle ensemble. Il y va de la défense de notre patrimoine, de celle de notre capital humain et numérique, mais aussi, demain, de notre vivre-ensemble. Tout ne doit pas être magique ni *made in USA*.

M. Patrick Chaize, rapporteur. – En tant que rapporteur chargé de l'examen du titre II du projet de loi, mon intervention sera centrée sur la

transposition de la directive 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, plus connue sous le nom de directive NIS 2.

À l'occasion d'un déplacement à Bruxelles effectué la semaine dernière, nous avons échangé avec des représentants de la direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne, la DG Connect, qui a piloté l'élaboration de cette nouvelle directive.

Pour le monde économique, les changements attendus sont significatifs dans toute l'Union européenne, mais plus particulièrement en France, puisque le nombre d'entités régulées devrait augmenter de 500 à 15 000 et celui des secteurs économiques concernés, de six à dix-huit, par rapport au précédent cadre de régulation défini par la directive NIS 1. Surtout, par principe, tous les systèmes d'information des entités régulées sont désormais concernés.

C'est un changement majeur de paradigme qui est à l'œuvre : il s'agit non plus uniquement de sécuriser des infrastructures critiques, mais d'assurer la résilience des entités critiques. Autrement dit, la couverture est bien plus large.

Plusieurs questions se posent auxquelles vous avez déjà esquissé quelques réponses.

Pensez-vous que les entreprises que vous représentez sont suffisamment informées des changements à venir ? Quel travail devrait-il être mis en œuvre pour y parvenir ?

Selon vous, l'Anssi est-elle suffisamment bien identifiée par le monde économique comme un interlocuteur de confiance dans le domaine de la cybersécurité ? Les entités régulées par la directive NIS 2 devront s'enregistrer auprès de l'Anssi, mais aussi lui signaler les incidents significatifs de cybersécurité ; il est donc important que l'Agence soit bien identifiée.

Parmi les entreprises que vous représentez, combien seront qualifiées d'entités essentielles, au titre de l'exercice d'une activité hautement critique, ou d'entités importantes, en raison de celui d'une activité critique ? Disposez-vous d'estimations précises ?

Le projet de loi confie, à juste titre, à l'Anssi des pouvoirs importants en matière de supervision, de contrôle des obligations des entreprises et de sanction en cas de manquement à ces obligations. Afin de permettre une application douce et progressive, seriez-vous favorable à la définition d'une période d'adaptation et d'accompagnement ? Vous avez répondu à cette question, pouvez-vous nous en dire davantage ? Les sanctions prévues vous semblent-elles proportionnées et adéquates ?

M. Hugues Saury, rapporteur. – Sénateur du Loiret, je siège au sein de cette commission spéciale en tant que rapporteur au titre de la commission des affaires étrangères, de la défense et des forces armées dont je suis membre. Aussi me revient-il d'instruire le titre Ier du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui transpose la directive REC en droit français.

Vous avez abordé différents sujets ayant trait aux moyens et à l'accompagnement, mais aussi à la proportionnalité et à la compétitivité. Mes questions recoupent ces sujets, mais aussi celles exprimées précédemment.

Quel bilan tirez-vous du dispositif actuel de sécurité des activités d'importance vitale ? Quel en est le poids pour les entreprises que vous représentez ? Celles-ci adhèrent-elles globalement à ce dispositif ? En la matière, leur intérêt peut varier selon l'importance des risques auxquels elles sont soumises.

Que pensez-vous de la philosophie générale de la directive REC et du titre Ier du projet de loi, notamment pour ce qui concerne la priorité donnée à la résilience plutôt qu'à la simple protection ?

Selon vous, les obligations prévues par le titre Ier – plan de résilience opérateur et plan particulier de résilience, notifications d'incidents, exigences spécifiques pour les entités critiques d'importance européenne particulière – sont-elles pertinentes et surtout proportionnées ?

Comment jugez-vous les mécanismes de contrôle et de sanction prévus en cas de manquements ou d'obstruction, notamment les plafonds, les procédures et les garanties associées ?

Avez-vous le sentiment que les dispositifs d'accompagnement proposés par l'Anssi répondent aux obligations énoncées par le projet de loi ?

Quel est le ressenti des acteurs de terrain ? Quelles sont les attentes des entreprises que vous représentez ?

Mme France Charruyer. – Pour répondre à M. Patrick Chaize et à sa première question sur l'état des lieux, selon les résultats de l'enquête que nous avons menée avec l'Ipsos sur la maturité des investissements cyber, un tiers des personnes interrogées avoue sa complète méconnaissance des questions réglementaires, quand un autre tiers souligne son manque de ressources humaines. Il existe donc un problème de compétences et un problème de moyens. Transformer l'entreprise au travers de la réglementation revient à la transformer en système autoapprenant, au sein duquel il faut intégrer la norme et faire monter en compétences les salariés. Par conséquent, le premier défi a trait à la formation. Les dispositifs d'incitation à la formation sont aussi des dispositifs de financement.

La deuxième question concerne la philosophie de la résilience et la directive Dora : cette réglementation est très intéressante puisqu'on parle enfin de remédiation, de résilience opérationnelle : actuellement certaines

directions des systèmes d'information font de la conformité en cochant des cases d'une documentation et en remplissant des formulaires, mais sans s'intéresser véritablement à la manière dont tout fonctionne sur le plan opérationnel.

L'enjeu est pourtant de savoir si la personne derrière le clavier, qui agit dans une interface homme-machine, est capable ou non de résister au biais d'automatisation et de se poser les bonnes questions lorsque cela est nécessaire. Les entreprises sont confrontées à une « polycrise », à une explosion des risques cyber et elles doivent s'outiller pour y faire face. Or dès lors que les menaces sont conçues par intelligence artificielle, il faut se doter aussi pour y répondre d'un outil d'IA. Tout repose alors *in fine* sur la qualité de la décision humaine : il importe de former les hommes placés dans une interface homme-machine à pouvoir toujours exercer leur esprit critique. C'est très concret : il faut avoir conscience que tout système informatique peut être craqué et que l'opérateur doit pouvoir reprendre la main face à la machine si cela est nécessaire.

Là où le bât blesse, c'est que prévaut toujours dans les entreprises, en ce qui concerne les obligations de déclaration et de notification, le « pas vu, pas pris ». Je vous renvoie au site de la Cnil sur les notifications de violations de données. Il est difficile, pour un dirigeant, de s'auto-incriminer. C'est compréhensible. La CPME a demandé à ses adhérents de vérifier si elles étaient soumises à NIS 2. Les dirigeants ne sont pas friands de « l'auto-incrimination » ; pourtant la procédure prévue est utile et le dispositif est très bon. Le risque est, paradoxalement, que les personnes préfèrent chercher à éviter d'appliquer la règle plutôt que de se poser les bonnes questions opérationnelles.

Vous me demandez si l'accompagnement de l'Anssi est suffisant. J'ai envie de vous dire qu'il ne sera jamais suffisant. Les CSIRT jouent un rôle crucial. L'offre de formation actuelle en matière de cybersécurité est surdimensionnée. Les entreprises sont conviées à de nombreuses conférences et à de nombreux ateliers sur la cybersécurité. Elles se voient proposées de nombreux outils très compliqués à base d'IA, mais l'ensemble est peu lisible. Cette offre semble surdimensionnée.

Or on nous demande, dans les contrats que l'on signe, d'être « à l'état de l'art », mais c'est très difficile. Cette notion n'est pas définie. Il faut avoir une très bonne connaissance des textes, des lignes directrices, savoir ce qu'est le Comité européen de la protection des données, savoir lire les décisions de justice, etc. Tout cela suppose de réaliser une veille documentaire importante. Qui peut faire ce travail ? Il me semble que cette tache revient aux CSIRT, qui travaillent en étroite collaboration avec l'Anssi et qui sont financés au niveau régional. La proximité est essentielle.

Nous ne recevons pas de messages d'alerte lorsqu'une faille de sécurité est détectée. Il conviendrait sans doute de revoir la législation et de

modifier la notion de recel de *leaks*, de réutilisation de fuites de données, afin de faciliter la détection des fuites de données et de permettre aux dirigeants de se saisir de cette problématique. Il faut que les PME puissent s'adresser à des tiers non marchands, dans les CSIRT, pour réaliser un diagnostic et déterminer si elles sont victimes de fuites. Elles ont besoin d'une formation et, surtout, d'une feuille de route pour se mettre à jour en matière de conformité. En effet, lorsque les petites entreprises travaillent avec des entreprises de taille intermédiaire (ETI) ou interviennent en tant que sous-traitants, elles sont soumises, comme leur donneur d'ordre, aux obligations définies par NIS 2. Il y a donc un enjeu de responsabilité.

Un autre enjeu concerne la gouvernance du risque. Les grosses entreprises, qui sont capables de gérer leur propre risque, doivent aussi scanner tous les risques existants dans leur chaîne de sous-traitants. Mais les petites entreprises, si elles sont victimes de fuites de données sans le savoir, ne comprendront pas pourquoi elles ne sont pas retenues dans un appel d'offres. C'est pourquoi les entreprises ont besoin des CSIRT.

La règle de proportionnalité est importante : si l'on veut mettre tout un écosystème au niveau, il faut être capable de descendre à l'échelle de tous les opérateurs, c'est-à-dire de faire en sorte qu'ils puissent s'appuyer sur des opérateurs de confiance, tel que les CSIRT, qui leur fournissent une aide en matière de cybersécurité conforme aux exigences de la réglementation, dans une relation non marchande. C'est ainsi que nous pourrons bâtir, dans les trois ans qui nous sont impartis, un écosystème performant. Notre but est de transformer ces centres en des entrepreneurs de la donnée. En effet, on ne peut pas s'intéresser à la réglementation sur la cybersécurité sans prendre en compte le contexte : le *Data Governance Act*, le *Data Act*, les appels à projets de Bpifrance sur la constitution d'entrepôts de données, etc. Notre seule richesse en ce domaine, en Europe, face aux Gafam, c'est notre créativité, notre agilité et notre capacité à travailler ensemble pour mettre en œuvre des mesures alternatives. C'est grâce à la mutualisation que nous pourrons avancer.

Mme Maxence Demerlé. – Je souscris aux propos qui viennent d'être tenus sur l'information des entreprises. Il est clair qu'elles manquent d'informations. La Commission supérieure du numérique et des postes (CSNP) avait d'ailleurs suggéré l'organisation d'une campagne d'information. Il conviendrait d'améliorer la communication sur toutes les questions relatives à la cybersécurité.

La plateforme Cybermalveillance a communiqué sur le sujet, en collaboration avec le Medef, en organisant le mois de la cybersécurité ou d'autres actions. Avec la CPME et l'U2P, nous avons créé le dispositif « Alerte cyber », sur le modèle d'« Alerte enlèvement », pour informer largement les entreprises en cas de découverte d'une faille de sécurité susceptible d'avoir des effets sur de nombreuses entreprises, alors qu'une solution simple à mettre en œuvre existe. Nous avons eu cette idée à la suite de l'affaire SolarWinds. Dans ce cadre nous avons relayé une douzaine d'alertes cyber en

deux ans ; nous avons sélectionné des cas très précis. Les alertes sont rédigées par Cybermalveillance et par l'Anssi et nous les diffusons ensuite au travers de notre réseau. J'espère que ce mécanisme a eu des effets, mais nous aurions besoin d'outils globaux à visée généraliste : les alertes publiées chaque jour par l'Anssi sur le site *www.cert.ssi.gouv.fr* ne sont pas compréhensibles, à moins d'être un expert. Un effort d'intermédiation s'impose. Il faudrait créer une sorte de météo de la cybersécurité, qui pourrait informer les entreprises des attaques les plus graves, face auxquelles elles peuvent réagir.

En outre, les *softwares* en vente sur le marché n'ont pas tous la même date de garantie en ce qui concerne la maintenance informatique de cybersécurité ; pour certains produits celle-ci est prévue jusqu'au 15 novembre 2027, pour d'autres elle va jusqu'en 2030, etc. Une grande diversité prévaut en la matière et ce n'est guère lisible pour les entreprises.

Nous avons donc besoin d'un effort de clarification et de mettre en œuvre des outils simples. Il faut que l'entrée en vigueur de ces directives soit accompagnée d'une grande campagne de communication.

À la différence de la CPME, nous ne demandons pas la création d'un service public de la cybersécurité, mais il est sans doute possible de mettre en place un système d'aide renforcée dans ce domaine, notamment en cette période de transition. La plateforme Cybermalveillance a créé un label ExperCyber : c'est un gage de confiance et d'indépendance. Il est important de disposer d'opérateurs spécialisés indépendants, qui même s'ils interviennent dans le secteur marchand, ont été labellisés par une entité qui n'a aucun intérêt commercial. Je regrette d'ailleurs que la communication autour de ce label n'ait pas été plus importante, car les entreprises ont besoin de savoir à qui elles peuvent s'adresser en toute confiance.

Les coûts de mise en conformité sont importants. J'ai été surprise en constatant que l'article 14 du projet de loi prévoyait que non seulement les coûts de mise en conformité, mais aussi les coûts liés aux contrôles de l'Anssi seraient à la charge des entreprises. Les coûts des contrôles de l'Urssaf ne sont pas à la charge des entreprises !

Les sanctions prévues sont aussi très élevées, pouvant aller jusqu'à l'interdiction d'exercer. Selon les termes de l'article 37, « la commission des sanctions peut interdire à toute personne physique exerçant les fonctions de dirigeant dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité, jusqu'à ce que l'entité essentielle ait remédié au manquement. » Nous sommes résolument opposés à cette disposition. Cette sanction est excessive. Les sanctions financières nous semblent déjà très élevées.

Je ne sais pas combien d'entreprises sont visées par la directive NIS2 : il est probable que la grande majorité des entités essentielles et des entités importantes sont membres du Medef, mais je n'ai pas de recensement et je ne sais pas quelles sont les entreprises concernées précisément. Le volet du projet

de loi correspondant à la directive REC est plus spécifique. Les entreprises qui étaient anciennement des opérateurs d'importance vitale (OIV) se sont habituées à la réglementation. Elles sont aguerries. Celles qui étaient considérées comme des opérateurs de services essentiels (OSE) sont, elles aussi bien habituées aux contraintes qui s'imposent à elles.

La notion de résilience est fondamentale. Un chef d'entreprise m'indiquait qu'il faisait des sauvegardes tous les deux jours et que celles-ci n'étaient pas sur le réseau. En cas de cyberattaque, il ne peut perdre, au pire, que deux jours de données. Voilà une démarche de résilience. Plus celle-ci est développée, moins les cyberattaques ont de conséquences. Attention toutefois à ne pas demander aux entreprises d'être des devins : elles ne peuvent pas tout anticiper !

M. Olivier Cadic, président. – Il n'y a pas de CSIRT dans toutes les régions et l'une d'entre elles n'a pas voulu en créer. L'Anssi a commencé à installer ce réseau lorsqu'elle disposait d'une certaine manne budgétaire lors de la crise du covid. Aujourd'hui, ces centres sont à la charge des régions. La question du financement se pose donc : nous devons vérifier si le modèle proposé est bien finançable. La question de la création d'un service public de la cybersécurité a été soulevée, mais il semble difficile, vu les contraintes budgétaires que l'on connaît actuellement, de mobiliser des crédits à cette fin.

M. Damien Michallet. – Alors que le RGPD s'inscrivait dans une approche plutôt punitive, la visée de ces directives est différente : il s'agit de renforcer la productivité et la compétitivité de nos entreprises. Nous devons veiller à les transposer strictement et à éviter toute surtransposition. L'enjeu économique est réel : autant il serait risqué de ne pas chercher à se prémunir contre les risques cyber, autant on pénaliserait la compétitivité de nos entreprises en alourdissant le texte et en surtransposant.

Vous avez évoqué les obligations liées à la mise en œuvre du RGPD, mais les entreprises doivent aussi mettre en œuvre les obligations prévues par la directive européenne relative à la publication d'informations en matière de durabilité par les entreprises (CSRD) ou concernant la généralisation de la facturation électronique : comment les entreprises font-elles face à toutes ces contraintes concomitantes ? Quel serait le coût pour les entreprises lié à l'entrée en vigueur de ce projet de loi ?

Mme Catherine Morin-Desailly. – La Normandie a été la première région à créer un CSIRT. Je suis donc très intéressée par vos propos sur ces organismes. L'aide des régions, en lien avec l'Anssi, est-elle utile aux entreprises ? L'échelon régional est-il, selon vous, l'échelon approprié pour vous apporter une réponse globale et coordonnée en la matière ? Que pensez-vous par ailleurs de l'articulation entre les CSIRT et les services spécialisés de police ou de gendarmerie ? Vous avez évoqué le RGPD. La Cnil est donc compétente aussi. Je viens de corédiger un rapport sur la dérive normative de l'Union européenne. Dans la lignée du rapport Draghi, nous montrons que

l'accumulation des normes pèse sur les entreprises. Comment réagissent-elles ? Il me semble avoir compris qu'elles appellent à davantage de communication en matière de cybersécurité, voire à la création d'un service public dédié, et à une montée en compétence numérique globale de la société, par le biais de la formation initiale ou de la formation continue.

Mme Audrey Linkenheld. – Je voulais aussi vous interroger sur les CSIRT. Les financements vous semblent-ils suffisants en matière de cybersécurité ? Que pensez-vous de l'articulation entre les CSIRT et les campus cyber ? Faut-il rapprocher davantage ces structures ? Vous avez dit aussi que les CSIRT avaient un rôle de lanceur d'alerte. Il me semble qu'ils ont pour mission de sensibiliser ou de répondre à des incidents. Pourriez-vous préciser vos propos sur ce point ?

La directive NIS 2 visera les entreprises mais aussi les collectivités. Le risque financier est très important pour une entreprise en cas de fuite de données ; la cyberattaque d'une entité publique peut avoir des effets vitaux pour la société – je pense notamment au secteur de la santé. Faut-il donc, comme le prévoit ce texte, traiter le secteur privé et le secteur public de la même manière ?

Mme France Charruyer– En ce qui concerne les campus cyber et les CSIRT, je vous répondrai en prenant l'exemple que je connais de l'Occitanie et de la Nouvelle-Aquitaine. Le campus cyber de la Nouvelle-Aquitaine est aussi un CSIRT. Le système fonctionne très bien. Nous sommes invités à participer à leurs travaux. Nous pouvons faire beaucoup de formations gratuites à destination des entreprises. L'essentiel, c'est l'échange de bonnes pratiques et la remontée d'informations.

Je connais le cas d'une entreprise qui a été victime d'un *ransomware*, mais cette attaque a touché aussi, par capillarité, 80 entreprises. Celles-ci n'avaient plus accès à leur logiciel de gestion des relations clients (CRM) et ne pouvaient plus facturer leurs clients. On a ainsi assisté à une cascade de défaillances d'entreprises. Une cyberattaque peut donc être létale pour les petites entreprises, car celles-ci n'ont pas une trésorerie importante. La défaillance d'un éditeur de logiciel peut avoir des effets dévastateurs sur les entreprises. Cela va très vite. Les entreprises n'ont pas le temps d'obtenir des aides. Certes les entreprises ont signalé le problème et se sont acquittées de leurs obligations de conformité, mais le temps économique n'est pas le temps réglementaire et elles ont été obligées de se déclarer en cessation de paiement. Plus les entreprises sont petites, plus elles sont vulnérables.

Les CSIRT font un effort de formation pour aider les entreprises à se transformer en systèmes autoapprenants et pour développer les échanges d'informations. Moins de la moitié des entreprises disposent de solutions de détection des menaces. C'est pourtant essentiel pour monter en gamme en matière de cybersécurité. Or les dispositifs puissants de détection des menaces sont souvent possédés par des organismes étatiques. L'article 24 du projet de

loi prévoit que l'Anssi sera compétente pour agréer les organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents. Si l'on souhaite conserver les CSIRT, avec un mécanisme de financement à imaginer, mais qui ne soit pas uniquement régional, il faut développer les échanges entre les ingénieurs de l'Anssi, les informaticiens des campus cyber, la police et la gendarmerie, etc. Dans le cas que j'ai évoqué, si la fuite de données avait été remontée plus tôt, il aurait peut-être été possible d'aider les entreprises à faire des sauvegardes et d'éviter la contagion. C'est une solution opérationnelle assez simple, mais pourquoi ne pas la mettre en œuvre dans la mesure où nous avons les outils et les hommes compétents ?

Faut-il prévoir des normes différentes pour le public et le privé ? Nous avons tous le même objectif : défendre la compétitivité du territoire. J'ai eu l'occasion de travailler avec Départements de France. Certains départements ont été touchés par des cyberattaques d'ampleur. Nous nous sommes tous réunis – directeurs des systèmes d'information, élus, directeurs juridiques – pour comprendre pourquoi il avait été possible de résoudre les problèmes rapidement dans certains départements et pourquoi cela avait été plus difficile ailleurs. Nous avons identifié des éléments très simples : on ne paie pas toujours les sous-traitants le même jour ; la personne qui a le chéquier n'est pas toujours la même ; dans certains cas, une cellule de crise a été constituée, etc.

Nous avons ainsi réussi, tous ensemble, à établir un plan de réponse aux incidents que nous avons envoyé à tous les acteurs. C'est pourquoi je parlais de « commun numérique ». Les départements n'ont pas d'argent. Leurs personnels ne sont pas toujours formés. Or lorsque l'on organise une formation pour dix personnes, il ne coûte rien de l'ouvrir à cent ! Il faut faire confiance à l'intelligence collective. L'essentiel donc, c'est que les CSIRT ou les campus cyber – peu importe le nom de la structure – permettent de mobiliser l'intelligence collective et de publier des documents utiles pour aider les directeurs des systèmes d'information des départements.

La nouvelle réglementation européenne est intéressante, car elle définit strictement les procédures. Son défaut tient au manque de clarté des définitions, et à la cacophonie en ce qui concerne les délais de déclaration des cyberincidents : par exemple, dans le cadre de la loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (Lopmi), l'indemnisation de pertes et dommages causés par une cyberattaque est subordonnée au dépôt d'une plainte dans les 72 heures. La distinction entre un incident de sécurité et une violation de données n'est pas aisée à comprendre. Le RGPD vise à défendre et à protéger les données. Le RIA vise à défendre l'innovation. Cette réglementation n'est pas un simple millefeuille. On en comprend l'esprit lorsque l'on met bout à bout tous les textes : elle traduit la volonté de remettre la main sur le patrimoine informationnel et de le valoriser. Cela implique de le protéger : c'est la logique des directives Dora, NIS 2, CSRD, etc. Il s'agit de faire moins, mais mieux. Dans le RGPD prévaut

le principe de minimisation des données, mais c'est aussi une question de soutenabilité. Ainsi il y a deux enjeux, de valorisation et de soutenabilité.

Il importe de comprendre comment fonctionne la réglementation. C'est ainsi que l'on peut éviter les redondances. Lorsque l'on demande aux entreprises de faire des analyses de risques sur le déploiement d'outils à base d'IA, il ne s'agit pas que les entreprises fassent une analyse d'impact RGPD, puis une analyse d'impact RIA. La présidente de la Cnil a dit très clairement, il y a deux semaines, qu'on allait faire en sorte d'éviter que les analyses de risques soient redondantes. La logique est bien celle d'une approche par les risques. Il s'agit de faire confiance aux opérateurs économiques pour qu'ils déterminent leurs bonnes pratiques. Le principe *d'accountability* rime avec responsabilisation.

La solution n'est pas l'empilement des normes. Ce qu'il faut, c'est que les acteurs travaillent ensemble au déploiement des bonnes pratiques opérationnelles. Les secteurs de la défense et du spatial ont besoin de bonnes pratiques particulières, ne serait-ce que pour s'adapter aux réglementations spécifiques. Dans ces domaines, nous parlons de technologies duales. L'intervention de l'Anssi est indispensable, comme celle de spécialistes. Il faut une réglementation « métier ».

On peut en dire autant des transports ou des données de santé. Il faut réfléchir à l'échelle sectorielle et renforcer la mutualisation dans un même secteur d'activité – c'est, au fond, une question de bon sens. On évitera ainsi que les incidents cyber et les violations de sécurité ne deviennent létales.

Mme Maxence Demerlé. – Comme Mme Charruyer, je crois profondément à l'intelligence collective et à la vertu des têtes de réseau. C'est précisément le rôle que nous avons essayé d'assumer.

Dans ce domaine, il a d'abord fallu faire feu de tout bois : diverses initiatives régionales ont émergé, se traduisant en particulier par le développement de campus, pour faire apparaître un écosystème d'entreprises. C'était là un préalable indispensable à la prise de conscience des enjeux de cybersécurité.

Passé cette période de grande créativité, l'heure est manifestement à la rationalisation. À ce titre, les CSIRT ne suffiront sans doute pas. Toutes les régions n'en disposent pas. Sauf erreur de ma part, la région Auvergne-Rhône-Alpes n'a pas créé une telle structure. Quant au CSIRT de Corse, il n'emploie que quelques personnes et, si compétentes soient-elles, un si faible effectif ne saurait suffire.

Nous avons besoin de têtes de réseau : c'est notre capacité à réagir collectivement qui importe. Pour autant, tout ne saurait être décidé depuis Paris. De nombreuses initiatives très créatives, venant des territoires, doivent être préservées.

J'y insiste, les dispositifs de ce texte reposent largement sur les entreprises elles-mêmes. Ces dernières doivent se notifier et se mettre en conformité. Ce sont elles qui assumeront le coût des contrôles et, le cas échéant, celui des sanctions. Or la responsabilité doit aussi relever d'un écosystème plus large. En ce sens, le label ExpertCyber peut être une bonne piste. De même, la création de systèmes d'information globale, axés sur la prévention, constitue un enjeu essentiel.

L'initiative de Départements de France est très intéressante à cet égard. Pour notre part, nous avons pris soin d'afficher, à chaque étage de notre siège, les cinq gestes à accomplir en cas d'attaque cyber, à côté des consignes à suivre en cas d'incendie. Nous nous sommes contentés de reprendre les recommandations de Cybermalveillance… La culture de la cybersécurité doit se diffuser partout, et un tel effort ne coûte pas forcément grand-chose.

La compétition entre réglementations a été évoquée. À ce titre, je vous le confirme : dans nos réseaux d'entreprises, nous avons plus entendu parler de la directive CSRD que de NIS 2, peut-être pour des raisons relevant de la communication. À mon sens, ces réglementations ne sont pas concurrentes. Il faut assurer leur articulation pour garantir la meilleure sécurité. Nous y gagnerons tous économiquement.

Nous avons aujourd'hui toutes les cartes en main. En particulier, nous pouvons compter sur de très belles entreprises de la cybersécurité : il faut leur donner un marché et les laisser travailler.

En la matière, le *benchmarking* a tout son sens. La Belgique, qui a déjà transposé la directive NIS 2, dispose d'une équivalence de conformité avec la norme ISO 27 001, qui est gage d'efficacité et de rapidité. Nous pourrions réfléchir à une disposition comparable. Les experts, notamment ceux de l'Anssi, ne jugeront peut-être pas une telle solution satisfaisante, mais il est urgent d'avancer. Alors que les labellisations sont nécessairement onéreuses, une telle présomption de conformité permettrait d'aider les entreprises en limitant les coûts.

M. Olivier Cadic, président. – J'abonde dans votre sens, car je ne suis pas du tout convaincu de la nécessité de légiférer dans ce domaine. Une loi n'a pas été nécessaire pour que les Français mettent des volets à leurs fenêtres et des serrures à leurs portes : pourquoi en faudrait-il une pour ajouter des pare-feu aux serveurs informatiques ?

Comme vous le soulignez, la Belgique a transposé la directive NIS 2 en retenant une approche très pragmatique. Le secteur de la cybercriminalité représente un chiffre d'affaires annuel de 1 500 à 2 000 milliards de dollars. On demande aux entreprises de payer pour se protéger à ce titre, mais l'État se doit, pour sa part, d'assurer la sécurité de tous, citoyens et entreprises confondus.

Bref, nous nous posons, comme vous, de nombreuses questions à ce sujet. C'est tout le sens du travail de réflexion que nous menons, en particulier, avec MM. les rapporteurs.

Mme Vanina Paoli-Gagin. – Un grand nombre de données que nous évoquons relèvent du *cloud*. À cet égard, l'absence de *cloud* souverain européen n'est-elle pas une faiblesse de l'édifice de protection numérique que nous nous efforçons de bâtir avec ce projet de loi ?

Mme Maxence Demerlé. – Il est possible qu'en vertu de ce projet de loi l'Anssi exige demain des entreprises qu'elles aient recours à des produits certifiés. En tout cas, la question se pose.

Pour sa part, le Medef souhaite garantir la plus grande liberté des entreprises. En ce sens, ces dernières doivent avant tout pouvoir faire un choix éclairé : c'est précisément pourquoi nous faisons de la transparence l'un de nos chevaux de bataille. Les entreprises doivent connaître les caractéristiques, notamment les contraintes techniques et juridiques, des produits qu'elles utilisent.

Aussi, le Medef s'est prononcé en juin dernier pour la labellisation dite EUCS +, assurant la transparence quant à l'application éventuelle de lois extraterritoriales. Nous sommes plusieurs organisations à militer en ce sens, même si certains pays de l'Union européenne s'y opposent.

Un groupement d'entreprises européennes s'est constitué de lui-même à cette fin. Dès lors que des entreprises réclament un tel niveau de labellisation, nous soutenons leur démarche. Mais, à nos yeux, cette labellisation ne doit pas être imposée : une entreprise doit pouvoir recourir au prestataire de *cloud* de son choix, dans les limites retenues par l'Anssi.

Mme France Charruyer. – Au sujet du *cloud*, un certain nombre d'enjeux nous échappent à l'évidence. Quant à la norme EUCS, elle risque malheureusement de ne pas être étendue dans le sens indiqué, du fait des luttes d'influence à l'œuvre au sein de l'Union européenne.

La liberté des entreprises est évidemment un enjeu majeur, mais nous faisons d'ores et déjà face à l'augmentation du coût des licences américaines. Nous devons donc trouver d'autres solutions que les *clouds* certifiés qui nous sont proposés. On peut sans doute faire plus petit, moins cher et plus soutenable.

Mme Catherine Morin-Desailly. – Gardons-nous de toute forme de dépendance étrangère, qu'il s'agisse des licences américaines ou du gaz russe.

M. Olivier Cadic, président. – Mesdames, messieurs, permettez-nous de vous remercier une nouvelle fois des réponses que vous nous avez apportées. Je vous rappelle que vous pouvez également nous faire parvenir une contribution écrite : vous alimenterez ce faisant le travail de nos rapporteurs.

2. Audition de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information

M. Olivier Cadic, président. – Nous poursuivons nos travaux sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité par l'audition de M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Monsieur le directeur général, je vous remercie de venir nous présenter les dispositions de ce texte relevant de votre administration. Votre venue est d'autant plus attendue que nous avons dû reporter l'audition de Mme Clara Chappaz, secrétaire d'État chargée de l'intelligence artificielle et du numérique, par laquelle nous devions ouvrir nos travaux le 9 décembre dernier.

Avec MM. Michel Canévet, Patrick Chaize et Hugues Saury, rapporteurs, nous nous sommes rendus la semaine dernière à Bruxelles. Nous nous y sommes entretenus avec les représentants de la Commission européenne et des autorités belges, qui ont d'ores et déjà engagé la transposition de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne, dite NIS 2.

Aujourd'hui, c'est à vous que revient la première prise de parole publique de l'administration française au sujet de cette transposition. Selon vous, qu'apportera ce travail en matière de résilience et de cybersécurité ? En outre, qu'impliquera-t-il pour les entreprises et les collectivités territoriales ?

Je rappelle que cette audition fait l'objet d'une captation vidéo retransmise en direct sur le site internet du Sénat, qui sera ensuite consultable à la demande.

Avant de vous céder la parole, je vous félicite du lancement officiel, ce matin même, du site 17Cyber, qui remplace Cybermalveillance. Peut-être reviendrez-vous également sur ce chantier.

M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information. – Avant tout, je tiens à saluer la constance avec laquelle le Sénat a soutenu le 17Cyber, dispositif qui s'inscrit pleinement dans la logique de ce projet de loi.

Je suis très honoré de vous présenter aujourd'hui le titre II du texte soumis à votre examen, titre dont l'Anssi a piloté la rédaction et dont elle pilotera également la mise en œuvre, si le Parlement l'y autorise.

Permettez-moi de revenir en quelques mots sur la genèse de ce travail.

Contrairement à ce que l'on pourrait croire, la directive NIS 2 n'est pas la suite de la directive NIS de 2016, transposée dans notre droit national en 2018 et désormais connue sous le nom de NIS 1.

La directive NIS 1 se contentait de prolonger le cadre national établi *via* la loi de programmation militaire (LPM) de 2013, régulant un certain nombre d'opérateurs d'importance vitale au titre de la défense et de la sécurité nationale. Cette directive avait étendu les dispositions de la LPM à quelques enjeux sociétaux et économiques en suivant la même logique : protéger des opérateurs stratégiques contre des menaces très ciblées, principalement étatiques.

Ces menaces étaient alors notre quotidien. Elles le sont toujours, mais d'autres phénomènes s'y sont ajoutés.

La directive NIS 2 trouve précisément sa source dans l'évolution du paysage de la menace. On a ainsi vu apparaître la menace dite systémique, liée au crime organisé et notamment aux rançongiciels. Paralysant des hôpitaux, des collectivités territoriales, des entreprises ou encore, plus récemment, des universités, un certain nombre d'attaques ont marqué les esprits. Elles ne sont pas menées par des États, mais par des activistes se prévalant de causes diverses et variées en cherchant surtout à se mettre en lumière.

Activistes et membres de la criminalité organisée ont en commun une approche totalement indiscriminée ; quiconque est susceptible de devenir, tôt ou tard, leur victime. Les quelques exemples que je viens de fournir en donnent l'illustration.

D'une certaine manière, les petits acteurs, qui jusqu'à présent échappaient à la menace, sont frappés de manière disproportionnée. Ces attaques ont des conséquences économiques et sociales inacceptables. Elles affectent aussi bien la marche des services publics que la vie des entreprises, allant jusqu'à provoquer des faillites.

Certes, cette menace n'est pas de nature étatique, mais plusieurs groupes incriminés n'en ont pas moins, à l'évidence, des liens avec des États. Si les groupes du crime organisé prospèrent ainsi, c'est parce que les États où ils sont implantés ne leur opposent pas de résistance. Une épée de Damoclès est donc suspendue au-dessus de nos têtes, car ces différents acteurs sont susceptibles de se coordonner, dans une perspective de durcissement de la situation géopolitique. Or cette situation pèse sur la liberté d'action de l'État français. La vulnérabilité généralisée de notre société et de notre économie à ce type d'attaques est désormais un enjeu du dialogue entre États.

Nous avons dressé ce constat avec nos partenaires de l'Union européenne, et c'est sur cette base qu'a été rédigée la directive NIS 2, portée sur les fonts baptismaux lors de la présidence française du Conseil de l'Union européenne (PFUE) et publiée à la fin de l'année 2022.

NIS 2 est la suite logique de NIS 1 pour ce qui est des entités dites essentielles, c'est-à-dire les acteurs les plus matures, soumis à des exigences élevées. Mais, surtout, NIS 2 crée un paradigme de régulation de plus petits acteurs. Ces « entités importantes », selon les termes de la directive, constitueront la grande majorité des nouveaux assujettis. Elles n'ont pas

vocation à être protégées contre la menace stratégique ciblée d'un service de renseignements étranger, mais elles sont malheureusement les victimes récurrentes, pour ne pas dire quotidiennes, d'une menace systémique.

Avec NIS 2, nous changeons donc clairement d'échelle – la France dénombre aujourd'hui 500 acteurs régulés ; demain, il y en aura potentiellement plus de 15 000 – et, surtout, nous changeons de paradigme. Je le répète, on entreprend également de contrer la menace non ciblée, dite systémique.

À cette fin, la logique de sanction évolue elle aussi. À l'évidence, les sanctions pénales, en vigueur jusqu'à présent, ne sont pas opérantes. Il faut passer à des sanctions administratives et financières, beaucoup plus efficaces, dans le droit fil du règlement général sur la protection des données (RGPD).

Je précise que ce changement de paradigme sort l'Anssi de sa zone de confort. *De facto*, notre agence est, comme tous les autres acteurs, confrontée à la menace systémique, mais nous n'avons jamais été en position de réguler les entités dites importantes.

C'est dans cet esprit que nous avons mené ce travail, en suivant quelques principes directeurs.

Premièrement, nous avons fait en sorte d'éviter les surtranspositions. Le texte dont vous êtes saisis assure une transposition sèche garantissant l'exercice de deux droits d'option, l'un pour les collectivités territoriales, l'autre pour les établissements d'enseignement. À ce titre, j'estime que nous avons fait des choix rationnels et raisonnables, d'ailleurs comparables à ceux opérés par les autres États membres.

Deuxièmement, nous avons suivi un principe de proportionnalité. Pour les acteurs essentiels, nous nous inscrivons dans le sillage de NIS 1 et du code de la défense. En revanche, les entités importantes représentent un champ nouveau ; nous avons dû veiller à fixer le bon niveau d'exigence, ni trop haut – ce ne serait pas réaliste économiquement – ni trop bas – des exigences trop faibles seraient en effet bien trop faciles à contourner.

Troisièmement, nous avons mené un travail de coconstruction tout à fait inédit pour l'Anssi. Depuis septembre 2023, nous avons consulté plus de soixante-dix fédérations professionnelles, ainsi que les onze principales associations d'élus et quatre fédérations de collectivités territoriales, abordant tour à tour différents points de la transposition.

Ce travail va encore s'intensifier. Dès janvier 2025, nous allons mener des consultations relatives au cadre réglementaire. Il s'agit notamment d'évaluer avec précision l'empreinte économique des mesures que nous préconisons – les estimations figurent dans le dossier qui vous a été transmis.

Pour de petites structures partant de zéro – ce n'est pas le cas de toutes –, l'investissement initial demandé serait de l'ordre de 100 000 à 200 000 euros, les frais récurrents représentant 10 % de la somme mobilisée au

départ. Pour les entités essentielles, les montants sont nécessairement plus élevés. Mais, quelle que soit la taille de la structure, l'investissement initial est dix fois inférieur au coût d'une cyberattaque ; le coût récurrent y est donc cent fois inférieur. Or la cyberattaque est pour ainsi dire une certitude, à long terme, pour toute entité qui ne se protégerait pas.

En parallèle, même si cela ne sautera sans doute pas aux yeux des lecteurs de ce projet de loi, nous nous sommes attaqués au millefeuille réglementaire.

Au fil des années, les dispositions se sont accumulées, notamment dans le code de la défense. Notre intention est de donner, grâce à ce projet de loi, un référentiel commun à l'ensemble des cadres réglementaires et législatifs relatifs à la cybersécurité, qu'il s'agisse des acteurs assujettis à NIS 2, des opérateurs d'importance vitale relevant du code de la défense ou des administrations publiques relevant, elles, du référentiel général de sécurité (RGS), créé par une ordonnance de 2005.

Nous faisons un premier effort en faveur de la simplification, tout en allant dans le sens de l'harmonisation à l'échelle de l'Union européenne. Bien sûr, tous les États membres n'ont pas vocation à faire de même en la matière, sinon NIS 2 ne serait pas une directive, mais un règlement. Il n'en faut pas moins aligner autant que possible les différents dispositifs. Cette harmonisation sera favorable aux entreprises concernées. Je pense notamment à celles dont l'activité se déploie dans plusieurs États membres.

À cette fin, le groupe de coopération NIS 2, constitué par la Commission européenne, est chargé d'alimenter un dialogue permanent. Les actions subséquentes de la Commission sont examinées dans ce cadre, notamment l'acte d'exécution pris l'été dernier pour fixer le cadre applicable aux infrastructures numériques.

D'autres États membres peuvent être source d'inspiration, parmi lesquels la Belgique, seul pays de l'Union européenne ayant à ce jour totalement transposé la directive NIS 2, l'Italie s'approchant il est vrai de ce but.

La Belgique joue manifestement un rôle précurseur. Elle devrait en ce sens essuyer un certain nombre de plâtres au profit de l'Union européenne tout entière. Je garde ces différents éléments à l'esprit, et je souligne qu'ils ont guidé certains choix relevant de l'équilibre entre mesures législatives et réglementaires. C'est également un enjeu de souplesse dans la mise en œuvre de ce cadre normatif.

À cet égard, la question des délais est évidemment centrale. Il faut poser le cadre législatif et réglementaire le plus tôt possible – c'est tout le sens du travail que nous menons pour préparer les textes d'application –, mais, une fois le cadre posé, il faudra aussi prendre le temps de l'implémentation.

J'en suis convaincu, trois ans au moins seront nécessaires avant d'exiger une conformité complète, compte tenu des délais d'investissement, de renouvellement des marchés et des contrats. Pour certaines exigences n'impliquant pas d'investissement, les délais seront sans doute plus courts – je table sur six mois environ pour les exigences d'enregistrement auprès de l'Anssi et de notification d'incidents. Mais, j'y insiste, la conformité aux mesures techniques prendra au moins trois ans. Ces délais de six mois et de trois ans font d'ailleurs consensus parmi les États membres dont j'ai pu consulter les représentants, qu'il s'agisse de la Belgique ou de l'Allemagne.

Un autre élément fait consensus, et le Conseil d'État l'a d'ailleurs confirmé dans son avis : un tel travail ne peut pas relever de la loi. C'est, passez-moi l'expression, un *bug* de la directive, laquelle ne fixe pas de délai de mise en application ou de mesure transitoire. Ce sujet est renvoyé au pouvoir réglementaire.

De plus, j'ai particulièrement à cœur de ne pas dénaturer le fonctionnement de l'Anssi. Notre agence est historiquement connue comme un « cyber pompier », et nous en sommes bien sûr fiers. Or on ne peut pas remplir un procès-verbal tout en éteignant l'incendie…

Quand l'Anssi vient secourir une victime, elle ne saurait laisser planer un quelconque doute quant aux poursuites ultérieures. C'est précisément pourquoi ce projet de loi crée une commission des sanctions, qui sera seule à même de juger des sanctions prises *in fine* selon les règles qui s'imposent, à commencer par le principe du contradictoire, les principes d'impartialité et de proportionnalité. Les processus de l'Anssi donneront lieu, quant à eux, à une réflexion d'ensemble : l'information qui circule entre les missions d'appui aux victimes et les missions de contrôle et d'instruction menées en amont de sanctions doit être dûment filtrée.

J'ai déjà insisté sur la nécessité de préserver de la souplesse : cet enjeu vaut aussi en matière de conformité. Nous entendons ainsi fixer de grands objectifs au titre de la réglementation pour les mesures techniques, qui seront une formule parmi d'autres. Les assujettis pourront proposer d'autres moyens d'atteindre les objectifs qui leur seront assignés, qu'il s'agisse des mesures techniques ou de la gouvernance.

Enfin, dans les trois ans que nous nous donnons pour créer ce cadre, le besoin d'accompagnement sera considérable. Tous les acteurs que nous avons consultés le soulignent.

En la matière, nous sommes face à un enjeu de financement ; je ne suis pas le plus légitime pour me prononcer sur ce point, et les circonstances ne s'y prêtent guère. Nous sommes également face à un enjeu de communication et de sensibilisation. Nous nous attelons à ce travail depuis déjà de nombreux mois, en partenariat avec les associations et les fédérations que nous avons consultées. Vos collègues députés et vous-mêmes pourrez bien sûr y être associés : nous sommes à votre disposition.

Il y a également des enjeux d'outillage. Le portail *monespacenis2.cyber.gouv.fr* a été mis en ligne en version bêta, en attendant la promulgation de la loi ; il tient compte des critères d'appréciation figurant dans le projet de loi afin que les entreprises puissent tester leur assujettissement ou non à la directive NIS 2. La plateforme *monaidecyber.ssi.gouv.fr* a pour finalité de mettre en relation des aidants et des entités afin d'établir un premier diagnostic non commercial des besoins de sécurité que celles-ci peuvent avoir.

Il existe ensuite un enjeu de mobilisation de tout l'écosystème, qu'il s'agisse des ministères dans leur rôle de coordination sectorielle, des organisations professionnelles, des acteurs comme le groupement d'intérêt public (GIP) Cybermalveillance, qui a une expérience remarquable dans l'accompagnement de plus petites structures, des relais locaux que sont les chambres de commerce et d'industrie, des agences de développement économique, des services de l'État du dernier kilomètre – la gendarmerie par exemple –, des CSIRT (*Computer Security Incident Response Team*) territoriaux...

À cela s'ajoutent un enjeu de développement et d'appui et un enjeu d'organisation. Il faudra poursuivre le débat sur la notion de guichet de notification d'incident, en gardant l'esprit que tout doit *in fine* remonter à l'Anssi, conformément à la fois à la directive et aux besoins de capitalisation sur la menace et de circulation de l'information. Il faudra toutefois veiller à ne pas créer la maison qui rend fou des *Douze Travaux d'Astérix*, mais au contraire faire en sorte que les victimes d'une cyberattaque soient accompagnées dans leurs démarches jusqu'à remplir l'obligation de notification et non pas renvoyées d'un guichet à un autre.

J'en viens à la question de l'adéquation des moyens de l'Anssi à l'objectif de mise en œuvre. Nous avons estimé le besoin global lié à la mise en œuvre de NIS 2 à 50 équivalents temps plein (ETP) dans une perspective triennale, en plus de la croissance triennale déjà actée de 40 ETP par an. Sans préjuger des débats qu'il reste à mener sur le projet de loi de finances pour 2025, il est évident que cela ne se fera pas l'année prochaine, comme il est évident que le calendrier de transposition a glissé. L'année 2025 sera donc consacrée à la définition et à la mise au point du cadre, qu'il s'agisse du parcours législatif ou de sa déclinaison réglementaire, ainsi qu'à l'amorçage de NIS 2. Nous y parviendrons en conservant la même enveloppe, par une bascule d'efforts et au détriment d'autres missions. Néanmoins, le besoin demeurera pour les années suivantes.

M. Olivier Cadic, président. – Lors de la table ronde avec les organisations professionnelles, qui vient de se tenir, le Mouvement des entreprises de France (Medef) et la Confédération des petites et moyennes entreprises (CPME) ont salué le travail de l'Anssi, mais déploré un manque d'information des entreprises à ce stade. Ils s'étonnent que l'article 14 fasse reposer le coût de son contrôle aux entreprises. Par ailleurs, l'interdiction d'exercer des fonctions de dirigeant paraît disproportionnée.

M. Patrick Chaize, rapporteur. – Les échanges que nous avons eus la semaine dernière avec vos homologues à l'occasion de notre déplacement à Bruxelles ont été instructifs et ont soulevé quelques questions supplémentaires.

Premièrement, pensez-vous que les entreprises, en particulier les TPE-PME exerçant des activités critiques, qui seront qualifiées d'entités importantes et qui n'étaient pas soumises à la directive NIS 1, sont suffisamment informées de l'évolution du cadre normatif induite par l'entrée en application de la directive NIS 2 ?

Deuxièmement, que répondez-vous aux chefs d'entreprise et aux fédérations professionnelles qui craignent une « surtransposition » par l'Anssi ? Même si vous nous avez déjà rassurés sur ce point, le doute est légitime, car de nombreuses dispositions du projet de loi devront être précisées par voie réglementaire.

Par exemple, alors que la directive NIS 1 recensait six secteurs d'activité que l'Union européenne avait jugés prioritaires en raison de leurs effets potentiellement systémiques, la France en avait ajouté six autres. Désormais, la directive NIS 2 énumère dix-huit secteurs d'activité, mais, dans la mesure où la liste des entités concernées sera fixée par décret, des inquiétudes se font jour sur le fait que des secteurs d'activité supplémentaires pourraient être concernés.

Troisièmement, pensez-vous que les sanctions prévues sont proportionnées ? Le défaut d'harmonisation des sanctions à l'échelon européen risque d'entraîner une concurrence entre États. Les États membres qui ont déjà transposé la directive NIS 2 ont prévu des sanctions inférieures à celles que prévoit le projet de loi. C'est notamment le cas de la Belgique : jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial hors taxes pour les entités essentielles et jusqu'à 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial hors taxes pour les entités importantes, les offices et les bureaux d'enregistrement.

Quatrièmement, quelle sera la philosophie de l'Anssi dans les premiers mois d'application de la loi visant à transposer la directive NIS 2 ? Sera-t-elle une autorité compréhensive et accompagnante à l'égard des entreprises ?

Cinquièmement, pourquoi ne pas avoir repris directement dans le projet de loi la définition des incidents de cybersécurité devant être notifiés à l'Anssi telle qu'elle figure dans la directive NIS 2 ?

En conséquence, pouvez-vous nous confirmer que les décrets d'application qui seront préparés par l'Anssi seront bien en phase avec les différentes notions d'incident définies aux articles 7 à 14 du règlement d'exécution du 17 octobre 2024, qui distingue notamment les incidents importants des incidents récurrents et fixe des critères différents selon le type d'acteurs concernés ?

M. Hugues Saury, rapporteur. – Sauf pour la défense, pourquoi avoir choisi de confier à une autorité unique, l'Anssi, la mise en œuvre de la politique gouvernementale en matière de sécurité des systèmes d'information, alors que ce choix n'était pas imposé par la directive NIS 2 ? Dans la mesure où le champ d'application de l'Anssi a évolué avec les directives, notamment par la présence d'acteurs économiques, ne serait-il pas logique de faire évoluer la gouvernance ?

Pourquoi l'article 6 du projet de loi ne reprend-il pas la définition de la notion d'incident de la directive NIS 2, pourtant essentielle ? Est-il prévu de s'appuyer sur le règlement d'exécution 2024/2690 du 17 octobre 2024 dans les textes réglementaires à venir ?

Les dispositions du titre II relatives à la cybersécurité ne sont pas codifiées. Le Conseil d'État estime que ce choix nuit à l'accessibilité de la norme. Pourquoi ne pas avoir, pour plus de clarté, intégré ces dispositions dans le code de la défense ?

Quel type de mesures pourraient être prises par le Premier ministre pour répondre aux crises majeures ou affectant la sécurité des systèmes d'information ? Quels critères pourraient être retenus pour la définition de ces événements ?

Par ailleurs, *quid* des consultations que l'Anssi mène depuis l'automne 2023 avec des acteurs de terrain pour préparer la transposition de NIS 2 ? L'Anssi se donne au moins trois ans pour la pleine application de cette directive. Quel accompagnement est prévu, notamment vis-à-vis des moins aguerris au risque de menace cyber ? Accorderez-vous une attention particulière aux sous-traitants des entreprises relevant de la directive sur la résilience des entités critiques, dite REC ?

Confirmez-vous qu'aucune sanction pour non-conformité à la directive NIS 2 ne sera appliquée dans un délai de trois ans ?

L'Anssi apparaît comme le chef d'orchestre. Comment parvenez-vous à mobiliser et à travailler avec tous les échelons, notamment les partenaires européens et territoriaux et les services de l'État ? Quelles limites rencontrez-vous et quelles améliorations doivent être envisagées ?

M. Patrick Chaize, rapporteur. – J'ai une dernière question. Quelles seront les missions des 50 ETP supplémentaires ?

M. Olivier Cadic, président. – Voici la question de Michel Canévet, rapporteur pour la commission des finances : qu'est-ce qui justifie que, dans le règlement Dora (*Digital Operational Resilience Act*), il soit envisagé d'intégrer les sociétés de financement dans les entreprises contraintes ? Avez-vous identifié au sein du secteur financier et de celui des assurances des faiblesses dans le domaine cyber ?

J'en viens à ma propre question. La directive NIS 2 encourage le recours à des normes et spécifications techniques européennes et

internationales et indique que les États membres peuvent prescrire des produits et services certifiés dans le cadre de schémas européens afin de démontrer la conformité à certaines exigences. La France fera-t-elle le choix de suivre cet encouragement et de recourir à des normes et spécifications techniques européennes et internationales ? Si oui, quelles seront les normes ou standards retenus parmi tous ceux qui existent ? Qui sera chargé de ces choix ?

M. Vincent Strubel. – Sur la question de l'information des entités, je partage largement le diagnostic posé par la CPME. Nous avons été aux côtés des entreprises qui ont rencontré des difficultés et il faudra être mobilisé pour aider tout le tissu de PME potentiellement concernées par le périmètre de la directive NIS 2. La communication et la sensibilisation seront donc des enjeux majeurs. À cette fin, il n'y a pas de levier unique.

Je crois profondément au rôle des fédérations professionnelles, notamment dans le cadre des consultations, tout comme au rôle des parlementaires pour porter ce message auprès du plus grand nombre. Il nous faut mobiliser toutes les formes de communication possible, en capitalisant sur ce que nous avons fait dans le cadre de la préparation des jeux Olympiques et Paralympiques, par exemple en trouvant des canaux de communication inhabituels – j'ai ainsi répondu à une interview dans *L'Équipe* afin de toucher les acteurs du monde du sport et de leur parler de cybersécurité.

J'en viens à ce qui relève du réglementaire et du législatif. Comme toujours, nous avons été guidés par des injonctions contradictoires entre le besoin légitime d'avoir un débat parlementaire sur les paramètres du nouveau cadre et la nécessité de conserver une forme de souplesse pour, à la fois, poursuivre des consultations avec les acteurs sur les points qui ne sont pas tranchés et s'inscrire dans une temporalité plus longue.

J'en suis convaincu, nous avons besoin de nous inspirer des exemples de nos partenaires européens qui en sont à des stades d'avancement de transposition différents, la Belgique particulièrement, mais également l'Allemagne et d'autres pays. Il nous faut garder cette forme de souplesse.

Il était évident que la notion d'incident, qui figurait dans la directive NIS 2, serait précisée par un acte d'exécution – il a été pris cet été. Nous avons donc fait le choix de ne pas l'inscrire dans la loi, et de garder plutôt le levier réglementaire. Nous procéderons éventuellement à quelques ajustements mineurs pour l'intégrer dans le cadre plus général des dispositions préexistantes, notamment en ce qui concerne les prestataires de services qualifiés, qui seront soumis à la même définition d'incident. Nous apporterons peut-être aussi des précisions pour en affiner l'interprétation. Reste que nous avons bien l'intention de reprendre cette définition et de l'intégrer.

De la même façon, nous comptons suivre les évolutions du cadre européen ou des décisions prises par nos partenaires. Le niveau réglementaire

nous permettra de poursuivre une forme d'harmonisation et d'itération pour améliorer le texte de manière rapide dans les années à venir.

Si nous souhaitons maintenir une autorité unique, alors que la directive ne l'impose pas, c'est d'abord parce que c'est ce modèle qui a marché pour la France depuis la création de l'Anssi en 2009. Nous faisons aussi bien que nos amis allemands avec trois fois moins de moyens. Cette frugalité et cette efficacité constituent un marqueur historique de l'Anssi. Le modèle centralisateur permet d'avoir un acteur au-dessus de la mêlée, qui intervient dans tous les champs, n'a pas d'autres missions et n'est pas soumis à des conflits d'intérêts. Il est bien ce chef d'orchestre naturel, comme vous l'avez souligné, monsieur Saury.

Ce rôle découle à la fois de la loi, du fait que nous sommes placés sous l'autorité du Premier ministre, ainsi que d'une forme d'expertise et d'efficacité : nous parvenons à coordonner l'action des services de l'État, des services déconcentrés, des acteurs de terrain et des acteurs du privé.

Nous en avons eu une nouvelle illustration ce matin avec le lancement de la plateforme 17Cyber.gouv.fr au sein du GIP Acyma (Action contre la cybermalveillance), qui permet de mobiliser d'autres acteurs en vue d'apporter des réponses aux besoins plus spécifiques de nos concitoyens notamment.

Sur les consultations, les retours sont assez homogènes. Les points d'attention et de mise en œuvre que j'ai mentionnés en tiennent compte. La question des délais est évidemment très prévalente. Celle de l'accompagnement l'est tout autant, ce qui nous conduit à accorder un temps suffisant, mais aussi à mobiliser tous les acteurs du relais qui peuvent aider et épauler.

Des travaux sont en cours sur l'accompagnement financier. Sur ce sujet également, les Belges sont un exemple inspirant pour mobiliser les leviers d'accompagnement existants, mais aussi pour rentabiliser la conformité à NIS 2 en l'inscrivant dans une démarche de labellisation ou dans un périmètre plus large. À titre d'exemple, les assureurs et le secteur bancaire pourraient s'appuyer sur la conformité à NIS 2 pour fonder leurs analyses de risques et ainsi donner un avantage aux acteurs qui respecteraient cette directive.

La question de la codification s'est posée. Il est apparu qu'aucun code n'était réellement naturel : ni le code de la défense, car le champ d'application de NIS 2 dépasse très largement les enjeux de défense nationale, ni d'autres codes.

J'en viens aux sanctions. Dans le projet de loi, le coût des contrôles a vocation à reposer sur les entités contrôlées, comme le prévoit déjà le cadre législatif actuel, notamment la loi de programmation militaire.

Dans la directive, le régime de contrôle est clairement différencié entre les entités importantes et les entités essentielles. Le contrôle des entités importantes ne peut avoir lieu que *ex post*. Une forte suspicion de non-conformité ou d'irrégularité est nécessaire pour déclencher un contrôle. Toutes ces entités n'ont pas vocation à être contrôlées de manière systématique. Ce serait, j'en conviens, insoutenable pour elles.

En matière de sanctions, l'ensemble des États membres se sont alignés sur les seuils prévus dans la directive, concernant notamment les pourcentages du chiffre d'affaires global, soit 2 % pour les entités essentielles et 1,4 % pour les entités importantes. L'objectif n'est pas d'être maximaliste dans tous les cas ; il est de faire des questions de cybersécurité un sujet de gouvernance au bon niveau dans les entités assujetties, c'est-à-dire au niveau des comités exécutifs.

Le but de ce régime de sanctions est de faire en sorte que ce sujet, perçu à tort comme étant purement technique et dépendant du seul directeur informatique d'une entreprise, relève désormais du directeur financier, du directeur des affaires juridiques et du patron. C'est précisément à ces niveaux que les décisions en matière d'investissements dans la sécurité ou de gestion des risques doivent être prises.

L'interdiction d'exercer des fonctions de dirigeant est une reprise de la directive, mais je ne nous vois pas aller jusque-là. NIS 1 prévoyait déjà des sanctions pénales, mais personne n'a jamais poursuivi un chef d'entreprise devant les tribunaux pour manquement à une obligation prévue dans cette directive.

Je reviens rapidement sur la philosophie d'accompagnement : elle s'appuie sur la mobilisation d'un ensemble de relais que j'ai précédemment mentionnés, sur de la communication proactive et sur la mobilisation des fédérations professionnelles. En outre, elle nécessite énormément de pédagogie pour accompagner la maturation des entités assujetties, grâce à des contrôles à blanc. Nous devons pour cela constituer un premier noyau de structures de contrôle et de supervision afin d'aller au contact des assujettis et de tester le régime de contrôle.

Vous m'avez beaucoup interrogé sur la Belgique : ce pays est pour nous une source d'inspiration, pas uniquement d'ailleurs s'agissant de la transposition de NIS 2. Nous nous concertons assez régulièrement et nous leur savons gré d'essuyer les plâtres et de guider nos choix. Pour autant, nos dispositions ne seront pas totalement alignées sur les leurs, notamment s'agissant des *cyber fundamentals*, les mesures techniques que les Belges mettent en œuvre pour répondre aux exigences de la directive NIS 2. Nos niveaux d'exigence sont comparables, mais nous ne privilégions pas, pour notre part, la reprise *stricto sensu* de la logique des *cyber fundamentals*.

Les mesures techniques, dont l'élaboration fait toujours l'objet de consultations, s'inscrivent, pour ce qui concerne les entités essentielles, dans

la continuité de ce qui a été fait au titre de la directive NIS 1 ou du code de la défense, afin d'éviter un changement brutal pour les acteurs ayant déjà investi dans la mise en conformité avec le texte précédent.

Pour les entités importantes, la question de l'alignement sur le dispositif belge se pose. La démarche de nos amis belges repose en partie sur la norme ISO 27001, en partie sur des compléments issus du NIST américain (*National Institute of Standards and Technology*). Il s'agit non pas d'une certification conforme à une norme préexistante prise *in extenso*, mais d'un montage *ad hoc.* Tous les États membres sont confrontés à la même réalité : il n'existe pas de norme préexistante conforme à NIS 2 qui puisse être prise sur étagère. La norme ISO 27001 ne traite pas tous les enjeux de gouvernance par exemple.

Par ailleurs, la norme ISO 27001 est un dispositif d'analyse des risques par l'entité qui la met en œuvre. Pour notre part, nous considérons que les entités importantes ne seront peut-être pas toutes en mesure de conduire leur propre analyse des risques, car cela nécessite une certaine maturité. Nous allons plutôt privilégier la conformité à des règles claires et simples, ne nécessitant pas un travail d'intégration et d'internalisation de la réflexion sur les risques et sur leurs déclinaisons. Il ne faut pas imposer un modèle de conformité unique. Au risque de m'avancer un peu, je n'exclus pas que, à terme, la labellisation *cyber fundamentals* belge ou d'autres dispositifs d'autres États membres puissent être reconnus en France comme un mode de conformité acceptable. Compte tenu de la variété des entités assujetties, un modèle unique ne pourra pas convenir à tout le monde. Il faut de la souplesse.

Je n'ai pas répondu à votre question sur Dora, qui relève selon moi du périmètre du ministère de l'économie et des finances. J'indique simplement que nous avons travaillé avec les futurs régulateurs de Dora, qu'il s'agisse de la Banque de France, de l'Autorité de contrôle prudentiel et de résolution (ACPR) ou de l'Autorité des marchés financiers (AMF) pour essayer d'harmoniser deux directives et deux cadres qui ont été négociés parallèlement par des acteurs différents et qui vont s'imposer, pour certains, conjointement. Certaines entreprises – et c'est malheureux – relèveront en effet pour une moitié de leur activité de Dora et pour l'autre moitié de NIS 2. L'harmonisation ne sera pas totale, mais nous continuerons d'être en lien étroit avec les autorités de contrôle pour limiter les déperditions d'énergie et les frictions.

J'en viens à la répartition des 50 ETP. L'essentiel de la mission de mise en œuvre de NIS 2 relève des compétences habituelles de l'Anssi, à l'exception de la mission de contrôle et de supervision, de pré-instruction de possibles sanctions, lesquelles seront décidées *in fine* par la commission indépendante des sanctions. Il s'agit d'un métier totalement nouveau pour nous, qui requiert une trentaine d'ETP. En outre, nous devons renforcer notre accompagnement des bénéficiaires, ne serait-ce que pour accroître la coordination avec les ministères, les différents secteurs d'activité et les autorités de régulation.

Enfin, nous devons renforcer notre présence dans les régions. Nous avons aujourd'hui un coordinateur dans chaque région métropolitaine et un pour l'ensemble des outre-mer.

M. Hugues Saury, rapporteur. – Je n'ai pas l'impression que vous ayez répondu à nos questions sur la gouvernance et sur la chaîne de sous-traitants des entreprises concernées par la directive REC.

M. Vincent Strubel. – En ce qui concerne la gouvernance, l'ambition est de préserver le modèle qui a été le nôtre jusqu'à présent, celui d'une autorité chef d'orchestre. L'Anssi intervient dans tous les champs de la cybersécurité, en coordination avec l'ensemble des acteurs. Elle est tour à tour opératrice, régulatrice, conductrice de politiques publiques. C'est ce qui fait sa force et la cohérence de son modèle.

Notre activité opérationnelle nous conduit à nous confronter quotidiennement aux meilleurs attaquants du monde et à mettre fin à leurs agissements quand ils s'en prennent à des entités françaises. Nous avons aussi une action dans le domaine de la régulation et de la coordination de politiques publiques. Ce modèle fonctionne. Je ne vois pas pourquoi il ne fonctionnerait pas avec des missions étendues dans le cadre de NIS 2.

Le traitement des sous-traitants est une part du problème que nous cherchons à résoudre avec NIS 2. Nous travaillons depuis des années à la sécurité de nos infrastructures les plus critiques, mais il est également nécessaire de sécuriser leurs chaînes de valeur pour éviter les défaillances en cascade qui, *in fine*, feraient tomber les infrastructures critiques. Je suis convaincu que, malgré le travail sur les chaînes de valeur, on oubliera toujours un acteur. Il est donc nécessaire de prévoir une sécurité de base étendue à l'ensemble du tissu économique.

Il est en particulier nécessaire de prendre en compte la chaîne de valeur numérique. À cet égard, j'attire votre attention sur le *Cyber Resilience Act*, qui est un règlement européen, et donc d'application directe, dont l'objet est de réguler les fournisseurs du numérique, c'est-à-dire les éditeurs de logiciels. Ce règlement est la deuxième face de la même pièce. Je me réjouis que ces deux textes arrivent en même temps et instaurent un équilibre entre, d'une part, les utilisateurs du numérique, qui entrent dans le champ de NIS 2 et qui ont porté jusqu'à présent la totalité des responsabilités en matière de cybersécurité, et, d'autre part, les fournisseurs du numérique, qui ont depuis longtemps, et parfois à tort, échappé à toute forme de responsabilité quand ils fournissaient des logiciels vulnérables.

Je ne me fais aucune illusion sur la capacité d'une petite entité régulée assujettie à NIS 2 à imposer des règles de conformité à son éditeur de logiciel ayant pignon sur rue et présent sur un marché mondial. En revanche, un acte réglementaire européen régulant l'ensemble du marché intérieur lui permettra d'imposer de telles règles.

Mme Catherine Morin-Desailly. – Quel est votre point de vue sur le règlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir ? La commission des affaires européennes du Sénat s'est beaucoup étonnée que le texte intervienne de manière si précipitée, sans aucune étude d'impact ni projet de financement.

Certaines mesures vont à l'encontre de l'organisation française, comme la création d'un centre opérationnel de sécurité à l'échelle nationale. Quelle est selon vous la bonne échelle pour organiser un tel centre d'aide et de réponse à nos entreprises et à nos collectivités ?

M. Vincent Strubel. – Je commencerai par la deuxième question. La bonne échelle, en fait, c'est d'articuler toutes les échelles entre elles. C'est déjà une réalité, d'ailleurs, puisqu'au niveau européen il existe une coordination technique, le *CSIRT Network*, qui relie les centres nationaux de réponse aux incidents des États membres – pour la France, c'est l'Anssi. Il existe aussi une coordination au niveau des directeurs d'agence : je fais partie du club CyCLONe (*Cyber Crisis Liaison Organisation Network*), qui rassemble mes homologues des 27 États membres. Ceux-ci font charnière, comme moi-même, entre la réalité technique traitée dans le *CSIRT Network* et les directives de nos autorités politiques, que nous avons vocation à informer dans la gestion des crises majeures.

Ces réseaux s'articulent assez naturellement avec l'échelon national. Nous avons d'ailleurs un maillage régional de CSIRT, et il y en a aussi dans les entreprises. L'Anssi joue ce rôle pour le Gouvernement et à l'échelon national, mais elle anime aussi une communauté de CSIRT. L'articulation de tous ces réseaux est bonne. Elle a d'ailleurs été une composante fondamentale de notre traitement des cyberattaques durant les jeux Olympiques et Paralympiques. Une fois de plus, l'Anssi est passée petit à petit de son rôle habituel de chef d'orchestre de la préparation à celui de tour de contrôle pendant le déroulement des jeux. Elle a mobilisé tous ces réseaux, nationaux et européens, pour alimenter ses partenaires, parfois les rassurer, en tout cas se coordonner pour le traitement des menaces qui débordaient nos frontières.

Ce qui ne fonctionnerait pas, c'est une grande agence supranationale. L'idée refait régulièrement surface, il faut la combattre car c'est une fausse bonne idée. Cela ne répondrait pas à la logique de proximité qui est nécessaire. Et cela contournerait un élément fondamental : le partage des responsabilités, prévu par les traités, entre l'échelon européen et l'échelon national. Les États membres restent responsables de leur sécurité nationale.

Cela dit, le règlement sur la cybersolidarité me semble aller dans le bon sens car il respecte ces lignes rouges. En tout cas, il a été soutenu par la France. Un certain nombre de nos remarques ont été prises en compte, afin de ne pas glisser subtilement vers cette fausse bonne idée d'une grande agence supranationale, par exemple. Ce texte organise une concertation entre les États

membres et crée la possibilité d'une entraide, ce qui est nécessaire et utile : nous ne pouvons pas faire abstraction de ce qui se passe chez nos voisins, et nous avons intérêt à pouvoir les aider, parce que ce qu'il se passe chez eux a des conséquences chez nous.

Imaginons, par exemple, une attaque sur le réseau de distribution électrique. Même si le réseau électrique français se porte parfaitement bien, il suffit que le réseau électrique allemand, belge ou de n'importe quel autre partenaire européen s'effondre suite à une cyberattaque pour que les conséquences se fassent sentir aussi au niveau national : tout cela est interconnecté, et nous avons besoin de pouvoir aider nos voisins – et peut-être aurons-nous un jour besoin de nous faire aider par eux.

À cet égard, le règlement sur la cybersolidarité crée un cadre efficace. Il ne crée pas des bataillons de cybercombattants européens, qui attendraient l'arme au pied qu'une crise se déclenche, mais il permet et encadre la mobilisation de prestataires privés. En somme, il reproduit au niveau européen un modèle qui fonctionne très bien au niveau national. Nous avons en effet été précurseurs dans la certification de prestataires privés intervenant de cette manière, en réponse à un incident. Honnêtement, je ne sais pas comment nous ferions si nous ne pouvions pas nous appuyer, de manière quotidienne, sur ces prestataires. Bien sûr, quand on touche au cœur du régalien, que ce soit par la nature de la victime ou de l'attaquant, c'est l'Anssi seule qui intervient. Dans tous les autres cas, elle intervient aux côtés de prestataires privés.

M. Olivier Cadic, président. – Vous avez eu des mots très chaleureux pour vos collègues belges, je suis sûr qu'ils apprécieront. Ils ont d'ailleurs été eux-mêmes très élogieux à l'égard de l'Anssi quand ils nous ont reçus la semaine dernière.

Vous dites que, sans reconnaître le *Cyber Fundamentals Framework*, nous considérerons une entreprise comme conforme à NIS 2 si elle l'est à *Cyber Fundamentals Framework.* Cela me va. Il existe une deuxième possibilité, proposée par les Belges : ISO 27001. Leur seule demande est que le certificateur soit reconnu par leur agence. Cela pourrait-il vous convenir, ou voyez-vous une faille dans le dispositif ? Une troisième méthodologie, pour eux, serait de permettre que des personnes issues du centre de cybersécurité belge viennent auditer directement l'entreprise, en facturant ce service. L'Anssi envisage-t-elle cette option ?

Le Medef a parlé tout à l'heure de l'article 11. Comment s'applique la directive sur les groupements de sociétés ? Certains s'étendent sur plusieurs pays…

Je termine en évoquant les choix des produits et services certifiés dans le cadre des schémas européens. Quels sont les schémas retenus ? Qui sera responsable de ces choix ? Quelle politique industrielle sera mise en place afin de développer des produits et services certifiés en nombre suffisant pour les

quelque 15 000 entités qui seront concernées par NIS 2 ? Sauf erreur, le projet de transposition de NIS 2 n'aborde pas ces sujets.

M. Vincent Strubel. – Je ne m'engage pas à reconnaître le label belge tel quel, mais nous devons poursuivre la réflexion pour progresser vers une reconnaissance croisée. Il n'y a pas de faiblesse dans ISO 27001, mais quelques manques relatifs à la gouvernance, qui sont comblés par nos amis belges. Je reproche simplement à cette méthode d'impliquer une analyse de risque effectuée par l'entité qui doit se faire labelliser.

Bien sûr, il sera au cœur de nos exigences, pour les entités essentielles, que celles-ci effectuent leur propre analyse de risque, en modélisant leur activité, en identifiant les facteurs de vulnérabilité, les enjeux, etc. C'est un travail très vertueux, mais coûteux. Et il ne correspond pas forcément à ce qu'on doit demander à une PME… D'ailleurs, pour un secteur d'activité donné, l'Anssi est à même de porter une appréciation relativement adaptée sur les risques. Mieux vaut donc donner à ces entreprises la recette de cuisine que je mentionnais tout à l'heure, c'est-à-dire une liste de mesures communes. Bien sûr, je jouerais contre mon camp si j'interdisais à ces acteurs de faire des analyses de risque. Mais je ne vais pas le leur imposer.

Je ne ferme pas la porte à l'idée d'audits portés par l'Anssi. Nos propres équipes d'audit sont extrêmement mobilisées sur les enjeux les plus cruciaux et les infrastructures les plus critiques : il faudrait donc faire appel, comme c'est notre pratique courante, à des prestataires privés. À cet égard, le cadre de certification Passi (prestataire d'audit de la sécurité des systèmes d'information), qui existe depuis 2014, et qui a été rénové récemment dans la perspective de NIS 2 pour porter un niveau d'exigence moindre, est un bon moyen de structurer une activité d'audit.

En revanche, je n'ai pas l'intention d'imposer dans NIS 2 le recours à des prestataires certifiés par l'Anssi. Ceux-ci correspondent à un niveau d'expertise et à des exigences particulièrement élevés. Nous travaillons à diversifier le paysage des prestataires, avec un niveau d'exigence moindre pour certains. Ceux-ci peuvent être un appui, mais ils ne seront pas assez nombreux, en tous cas dans un calendrier compatible avec la mise en œuvre de NIS 2.

Il s'agit de valoriser le recours à des prestataires certifiés ou qualifiés par l'Anssi, en utilisant la notion de présomption de conformité : lorsque l'audit est mené par un prestataire certifié par l'Anssi, celle-ci ne posera pas de questions, dans sa mission de contrôle éventuelle, sur la qualité ou la nature de l'audit qui a été mené. Nous le prendrons pour argent comptant. Les experts cyber, par exemple, sont des prestataires sélectionnés avec un niveau d'exigence moindre, labellisé par nos collègues du GIP Cybermalveillance. Il serait dommage de se priver de ces acteurs, car ils peuvent suffire pour aider une PME à se protéger contre la menace ambiante, qu'on appelle systémique.

M. Olivier Cadic, président. – Merci pour ces précisions. Nous allons avoir un point d'entrée unique, qui répartira entreprises et particuliers vers le bon prestataire. La Commission le réclame depuis longtemps. Votre approche est axée sur l'entreprise et le client, c'est-à-dire qu'elle se focalise, à juste titre, sur la victime potentielle. Il n'est pas impossible que nous demandions à vous entendre de nouveau en fin de processus.

JEUDI 23 JANVIER 2025

Table ronde avec des organisations professionnelles de la cybersécurité (Alliance pour la confiance numérique, Clusif, CyberCercle, CyberTaskForce)

M. Olivier Cadic, président. – Nous poursuivons notre cycle d'auditions publiques consacrées au projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Je rappelle que notre commission spéciale s'est constituée le 12 novembre dernier pour examiner ce texte qui vise la transposition de trois directives : la directive sur la résilience des entités critiques, dite « REC » ; la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS 2 » ; et la directive qui concerne la résilience opérationnelle numérique du secteur financier, dite « DORA ».

Nous accueillons des organisations professionnelles de la cybersécurité : l'Alliance pour la confiance numérique, représenté par son président, M. Daniel Le Coguic, ainsi que M. Yoan Kassianides, Mme Elsa Auriol et M. Farid Lahlou ; le Clusif, qui est l'association de la sécurité du numérique en France, représenté par M. Benjamin Leroux ; le CyberCercle, représenté par MM. Christian Daviot, Stéphane Meynet et François Coupez ; et la CyberTaskForce, représentée par MM. Sébastien Garnault, Philippe Luc et Mme Anne Elise Jolicart.

Je vous remercie d'avoir répondu à notre invitation pour partager votre point de vue sur le projet de loi et l'impact de cette transposition pour les entreprises. Nous serons en particulier intéressés par les dispositions du texte qui vous posent problème et vos éventuelles propositions d'amendement. Nous pourrons ainsi relayer vos préoccupations à la ministre chargée de l'Intelligence artificielle et du Numérique, Mme Clara Chappaz, que nous entendrons lundi prochain.

Je rappelle à tous que cette audition fait l'objet d'une captation vidéo qui est retransmise sur le site internet du Sénat puis consultable en vidéo à la demande.

Vous représentez l'écosystème, vous m'apportez beaucoup dans mes travaux de rapporteur budgétaire, votre analyse nous est très utile, elle nous fait travailler différemment car nous ne nous contentons pas de consulter l'administration. Vos propos sont très attendus, ne vous limitez pas, en particulier sur le budget de l'Agence nationale de la sécurité des systèmes d'information (Anssi), nous sommes là pour vous écouter.

M. Daniel Le Coguic, président de l'Alliance pour la confiance numérique. – L'Alliance pour la confiance numérique représente les entreprises françaises dans le domaine de l'identité numérique, la cybersécurité, l'intelligence artificielle et les infrastructures de confiance.

Nous saluons le regroupement dans le même projet de la transposition de la réglementation européenne, de Dora et de NIS 2, ce qui simplifie notre vie et la discussion que nous souhaitons avoir avec la représentation nationale.

Nous sommes doublement intéressés par cette transposition : un certain nombre d'entreprises de notre syndicat sont directement concernées et vont mettre en œuvre les règles nouvelles, et notre organisation, de par son rôle dans la cybersécurité, souhaite continuer à coopérer.

Au-delà des aspects légaux, notre objectif est d'augmenter la résilience de la Nation. Nos adhérents nous disent et leurs clients le disent aussi, sur l'ensemble du territoire, il y a une inquiétude face à l'évolution du numérique – et ces directives ont pour vocation de mieux protéger nos organisations et nos concitoyens, en particulier les plus vulnérables.

Notre syndicat a déjà contribué en amont, avec l'Anssi et les institutions européennes, nous avons fait une analyse détaillée des directives en novembre 2023. Nous avons des propositions d'amendements que nous vous transmettrons et nous souhaitons continuer à être associés à la transposition, notamment dans la rédaction des amendements et des décrets.

Comment continuer dans ce sens ? Nous proposons d'installer une instance commune entre les parties prenantes, les cibles de la transposition, les acteurs industriels et économiques, pour coconstruire les règles et suivre leur mise en place, qui va prendre plusieurs années – cette instance commune est un facteur de succès pour atteindre nos objectifs.

Ensuite, nous proposons d'accompagner la transposition par un plan de sensibilisation et de communication auprès des cibles de la directive : la cybersécurité n'est pas suffisamment connue, il faut en faire comprendre les enjeux, au-delà des aspects techniques, il faudra des moyens spécifiques pour cette communication. La divulgation des vulnérabilités est importante, il faut en faire prendre conscience, échanger sur les problèmes et leurs solutions.

Enfin, nous appelons à valoriser l'expertise et les capacités technologiques de l'industrie française. Ces directives n'ont pas qu'un enjeu réglementaire, il faut mettre en place des solutions techniques et nous

souhaitons que les entreprises françaises y participent au premier chef, il faut leur faire une place, en particulier dans le cadre de la commande publique, c'est possible via l'Union des groupements d'achats publics (Ugap) et UniHA par exemple, c'est important dans la mise en œuvre.

M. Benjamin Leroux, membre de l'association Le Clusif. – L'association Le Clusif, reconnue d'utilité publique, regroupe des utilisateurs et des industriels, qui fournissent des services, je suis à son conseil d'administration et aussi directeur de la société Advens, spécialisée dans la cybersécurité.

Les directives à transcrire vont dans le bon sens. Nous sommes face à une menace importante, la question aujourd'hui n'est pas de savoir si l'on peut être attaqué, mais quand – et il faut augmenter notre protection et notre résilience, très largement. Le point positif de NIS 2 est le passage à l'échelle géopolitique. On avait une approche centrée sur les organismes d'importance vitale, mais désormais tout le monde peut être attaqué ; on a donc besoin d'élargir la couverture, en particulier en France, que ce soit dans la sphère publique ou privée. Beaucoup d'attaques sont le fait de petits cyberattaquants, elles peuvent avoir des effets graves sur des PME ou des structures publiques, alors qu'il n'est pas très difficile de s'en protéger – parce que ces petits cyberattaquants, en réalité, ne sont pas très doués. Il faut que la menace soit perçue par tout le monde.

Il y a une incidence de coût, certes, mais ce coût est raisonnable par rapport à celui de l'attaque – celle contre l'hôpital de Corbeil-Essonnes, par exemple, a coûté plusieurs millions d'euros : l'attaque est toujours plus coûteuse que la protection.

Mais pour réussir, il y a plusieurs facteurs à prendre en compte. D'abord, il faut élargir le nombre d'acteurs, donc faire faire de la sécurité à des acteurs qui ne se sentent pas concernés, il faut parler besoins humains, besoins de recrutement, il va falloir aussi former des responsables de cybersécurité, partout dans le territoire.

Autre point, nous avons besoin de définitions précises, certains termes font débat, il faut avoir les idées claires sur ce qu'est un incident, une vulnérabilité et le risque cyber – autant de termes abstraits pour les personnes non initiées. Avant les Jeux Olympiques, on parlait d'un risque de millions, voire de milliards d'attaques cyber, le bilan de l'Anssi fait état d'événements de sécurité qui se comptent par dizaines, ou par centaines. Il faudra donc trouver des termes consensuels qui parlent à tout le monde, pour que les structures concernées, quelle que soit leur maturité, mettent en place des mesures adaptées et proportionnelles pour atteindre un niveau global de résilience. Cela doit se faire à un coût raisonnable, en tenant compte des moyens de chacun. La réussite passera par la communication, la sensibilisation, le développement de la filière cyber, et de la précision pour que les personnes concernées soient à l'aise avec ces concepts parfois nouveaux.

M. Sébastien Garnault, fondateur de la CyberTaskForce. – Tout le monde dit que la directive NIS 2 est une opportunité, mais pour qui et pour quoi ? Nous répondons qu'elle doit bénéficier d'abord aux gens, mais cela demande un changement de paradigme. NIS 2 va réguler les organisations et pas les systèmes d'information, ce qui aura des conséquences concrètes sur les définitions – je partage ce qui vient d'être dit sur le besoin de définitions, en y ajoutant une dimension européenne : il faut que nous ayons des définitions communes avec nos voisins, ou bien nous ne nous comprendrons pas.

La transposition doit renforcer la résilience, cela va dans le bon sens. Cependant, le projet de loi ne fait pas de place à l'humain, aux gens, sauf pour des sanctions. Or, on le sait, les cyberattaquants passent par les personnes, on l'a vu à l'Assemblée nationale : les cyberattaquants n'entrent pas frontalement dans le système informatique, ils ont attaqué des députés en hackant leur téléphone.

Certains mettent en avant le coût de la protection, c'est une réalité. Mais il faut arriver à l'inclure dans le coût du système, avoir une approche *by design* – quand j'achète une voiture, je n'ai pas à y ajouter des ceintures de sécurité, elles sont déjà dans la voiture… Il faut de l'argent pour équiper les hôpitaux, ils ne sont guère protégés contre le risque cyber.

On évoque souvent la surtransposition, je dirais qu'ici, on risque plutôt une sous-transposition : c'est pourquoi je demande à ce qu'on couvre l'intégralité du champ, donc les systèmes et les gens – mais je laisse mon collègue Philippe Luc en parler.

M. Philippe Luc, membre de la CyberTaskForce. – Pour observer la menace cyber depuis près de vingt ans, je suis très sensible à la question des vulnérabilités humaines dans le risque cyber, et à sa place dans les systèmes de défense – c'est l'objet de l'entreprise que j'ai cofondée et que je dirige, Anozr way. Nis2 renforce les définitions, Dora intègre le facteur humain, les risques d'erreurs humaines – on devrait pouvoir mieux contrer toutes ces attaques par ruse, comme le *phishing*, le *smishing*, les attaques par SMS, l'usurpation d'identité, les *deepfakes*, l'espionnage, la déstabilisation, la manipulation, toutes ces attaques qui utilisent les données, notre exposition numérique, pour nous tromper dans le but de nous abuser, de nuire à nos entreprises, à nous-mêmes en tant que citoyens.

Pourtant, le facteur humain n'est pas abordé dans le projet de loi de transposition. On ne traite que des vulnérabilités techniques, alors que le facteur humain représente 80 % des attaques dans le monde cyber, il est le chemin d'accès le plus évident pour les attaquants. Or, plusieurs de nos voisins ont repris la définition de vulnérabilité inscrite dans la directive NIS 2, qui intègre les vulnérabilités humaines. Les Italiens ont défini la notion d'approche tous risques, les Allemands ont également privilégié cette approche, les Belges ont repris la définition intégrale de la directive.

Je vous citerai, Monsieur le Président Cadic : « Cette course pour se protéger des attaques cyber est une course sans fin et on n'en a pas les moyens. Il faut donc changer de paradigme et réfléchir différemment. » Je le pense également, et c'est pourquoi je penche pour une approche systémique, en regardant du côté des attaquants. Or, que font les cyberattaquants ? Ils commencent toujours par une phase de reconnaissance, qui inclut des étapes de vulnérabilité humaine. La matière première des attaquants, ce sont nos données, ils font du renseignement d'origine source ouverte – de l'*open source intelligence*, ou *OSINT*, en anglais –, une discipline qui n'est pas encadrée légalement et que nous avons intérêt à maitriser pour nous défendre. Pour se défendre, il faut penser comme des attaquants et regarder ce qu'ils voient – Sun Tzu : « Connais ton ennemi, mais connais-toi aussi toi-même. » La solution, me semble-t-il, passe par l'activité de veille et le renseignement d'origine source ouverte – beaucoup plus que par la sanction. Car attention, on parle beaucoup des sanctions prévues par NIS 2, il faut y réfléchir à deux fois : des entreprises vont dépenser de l'argent pour se protéger, mais on va les sanctionner quand elles seront victimes d'attaques, alors que même les grands groupes, malgré leurs moyens, peuvent être victimes d'attaques, en particulier par l'exploitation de données personnelles. Quels sont les moyens prévus pour contrebalancer ces sanctions ? Quels sont les moyens donnés aux forces de l'ordre et aux équipes de cybersécurité pour diminuer le risque ? Je suis convaincu que le renseignement d'origine source ouverte fait partie de la réponse.

M. Olivier Cadic, président. – Ce n'est effectivement pas en ajoutant toujours plus d'argent qu'on gagnera nécessairement la guerre – et, pour anticiper, il faut comprendre l'adversaire…

M. Christian Daviot, membre du CyberCercle. – Le CyberCercle rassemble depuis 2012 des acteurs économiques, des administrations et des élus, il a débattu plusieurs fois du projet de loi dont nous parlons aujourd'hui. Nous partageons les objectifs de cyber-résilience portés par les directives, étant très au fait des risques numériques des entreprises et des collectivités territoriales, ainsi que de leurs faibles capacités à y faire face.

Dans le temps qui m'est imparti, je soulignerai les flous de ce texte, qui peuvent être des loups, et je vous proposerai quelques pistes de bon sens, dont nous vous proposerons le détail par écrit, sachant que mon propos est issu des débats que nous avons eu au sein du Cybercercle.

Il y a un flou, d'abord, sur le champ d'application du texte. Si la directive NIS 2 fixe des secteurs d'activité, les critères de désignation des entités essentielles ou importantes sont à la discrétion des États membres. La directive prévoit de cumuler les chiffres de l'entité, le personnel, le chiffre d'affaires, le bilan, avec une partie de ceux des sociétés du groupe auxquelles l'entité appartient – mais elle donne aussi la possibilité aux États membres de prendre en compte uniquement les chiffres de l'entité si les systèmes d'information utilisés par cette entité dans le périmètre de NIS 2 sont

indépendants de ceux du groupe. Cette option n'étant pas intégrée dans le projet de loi, toute entité d'un groupe sera donc vraisemblablement considérée comme une grande entreprise, quelle que soit sa taille réelle, ce qui est un problème.

L'article 8 du projet de loi dispose qu'un décret en Conseil d'État confiera au Premier ministre le soin de désigner par arrêté les entités publiques soumises à la réglementation, sans plus de précision. Le projet de loi renvoie par 29 fois à des décrets en Conseil d'État, ce qui n'apporte pas de sécurité juridique aux entités visées. Personne ne peut dire combien d'entités seront concernées, d'autant qu'il y aura nécessairement une extension de l'application aux sous-traitants par la voie contractuelle. Nous serons donc bien au-delà des 15 000 entités annoncées.

Il y a un flou, aussi, sur les coûts à la charge des entités visées. Le coût moyen de mise en conformité était estimé à 400 000 euros dans la note du 15 mars 2024, mais le directeur général de l'Anssi a parlé de 200 000 euros devant votre commission spéciale. Ces coûts moyens sont relatifs à la seule transposition de NIS 2, REC et Dora. Il nous semble délicat de demander de telles dépenses au motif qu'une attaque couterait plus cher. Ensuite, on fait comme si l'entité était toujours incapable d'effectuer une analyse de risque, ce n'est pas le quotidien des dirigeants d'entreprises ni de toutes les collectivités territoriales. Selon les chiffres avancés, le coût global à la charge des entités visées oscillerait entre 3 et 6 milliards d'euros, c'est considérable et cela n'irait pas sans répercussion sur le coût des produits et services.

Il y a également un flou à propos des sanctions. Le Conseil d'État estime que si l'on exclut les collectivités territoriales des sanctions, il y a rupture d'égalité et obstacle à l'atteinte des objectifs de NIS 2. Les sanctions visant les dirigeants d'entreprises seront dans la loi, mais il a été indiqué qu'elles ne seront pas appliquées. Dire qu'il n'y aura pas d'interdiction de gestion temporaire, cela vide de sens la commission des sanctions. Nous nous interrogeons aussi sur sa composition, nous aurons des amendements.

Le rôle de l'Anssi comporte aussi du flou. Le Conseil d'État suggère que le Premier ministre puisse nommer une autre autorité pour contrôler les opérateurs, mais les missions de l'Anssi n'étant pas modifiées, cette possibilité reste théorique. Il est paradoxal d'affirmer que l'Anssi concentrera ses interventions sur les entités essentielles et vouloir y centraliser l'ensemble des procédures relatives aux entités importantes. La cybersécurité étant liée au métier, il faut donner un rôle aux ministères coordonnateurs des secteurs d'activité concernés et au tissu institutionnel et économique de proximité.

Il y a un flou, encore, dans la partie de l'étude d'impact relative à la transposition de NIS 2. Le Conseil national d'évaluation des normes a donné un avis négatif sur tous les articles pour lesquels il était consulté, mais l'étude d'impact n'en donne pas les raisons.

Nous avons trouvé également des loups dans ce projet de loi de transposition.

Toutes les parties prenantes sont attentives à la surtransposition des directives, mais nous sommes souvent moins attentifs à la sous-transposition, alors qu'elle est ici significative et qu'elle porte sur des enjeux majeurs. Ainsi, ce projet de loi ne reprend que deux des quatre objectifs fixés par l'article 2 de la directive NIS 2. La directive demande aux États membres d'adopter une stratégie nationale de cybersécurité et de la réviser tous les cinq ans : cela n'apparait pas dans la transposition. Un projet de stratégie existe mais il n'a pas été rendu public, nous avons pu le consulter, et voir qu'il ne reprenait pas les objectifs de la directive.

Le projet de loi ne reprend pas non plus les dispositions relatives aux règles et obligations pour le partage d'informations en matière de cybersécurité, prévues pourtant à l'article 29 de la directive. De même, le projet de loi ne reprend pas la définition d'un incident, qui figure à l'article 6 de la directive NIS 2. Cela peut avoir des conséquences, comme en 2002, où le choix de ne pas transposer la définition de l'expression « support durable » a compliqué la situation des opérateurs économiques. La Belgique, elle, a transposé intégralement cet article 6.

Nous vous proposerons en conséquence des pistes de bon sens, que je vous présente ici très succinctement – et que nous vous enverrons par écrit.

Nos amendements, d'abord, viseront à transposer l'article 4 de la directive REC et l'article 7 de la directive NIS 2 relatifs aux stratégies, l'article 29 de NIS 2 relatif aux accords de partage d'informations en matière de cybersécurité. Nous vous proposerons d'amender l'article 5 relatif à l'Anssi, l'article 6 pour intégrer la définition d'un incident, les articles 8, 10 et 11 pour préciser les entités visées, l'article 37 pour préciser les sanctions.

Nous vous proposerons, enfin, une piste de méthode pour appliquer ces règles nouvelles au plus près des acteurs économiques, en confiant aux ministères sectoriels une part de la définition des entités concernées – c'est l'article 12 du projet de loi –, mais aussi dans la définition des référentiels de contrôle de conformité. La démarche du ministère des Armées pour les entreprises relevant de la base industrielle et technologique de défense (BITD) nous semble exemplaire, elle pourrait être déclinée dans les secteurs d'activité visés par NIS 2. Enfin, nous suggérons d'ajouter un représentant du ministère coordonnateur du secteur d'activité auquel appartient l'entité mise en cause et d'un représentant de la branche professionnelle de ce secteur à la commission des sanctions, afin que les sanctions prises prennent en compte toute considération utile.

M. Olivier Cadic, président. – Merci pour ces propositions.

M. Michel Canévet, rapporteur pour la commission des finances. – Je suis particulièrement intéressé par la directive Dora, qui aurait dû entrer en application la semaine dernière, elle est un peu en retard, cela tient à l'absence

de normes techniques réglementaires (RTS) et de certaines conditions de mise en œuvre. Avez-vous des informations sur les éléments communiqués aux tiers par l'Autorité des marchés financiers (AMF) ou par l'Autorité de contrôle prudentiel et de résolution (ACPR) ?

La directive Dora semble surtransposer les règles concernant les sociétés de financement, notamment pour ce qui concerne le *leasing* et l'affacturage : avez-vous des échos dans ce sens ? Ne faudrait-il pas adopter une approche mieux proportionnée en fonction des acteurs ?

Un prestataire doit être opérationnel. Or, l'écosystème est pour une grande part d'origine américaine. Est-il possible de développer un écosystème français ou européen, et de réduire notre dépendance à l'égard des Américains ?

Enfin, les régulateurs devront faire du *reporting* en permanence. Si l'Anssi est équipée pour assurer une couverture permanente, ce n'est pas le cas de l'ACPR ni de l'AMF : des évolutions vous semblent-elles nécessaires ?

Des entreprises sont soumises aux prescriptions de Dora et à celles de NIS 2. Ces charges ne sont-elles pas excessives et l'application des deux directives ne conduit-elle pas à une sur-réglementation ?

M. Patrick Chaize, rapporteur pour la commission des affaires économiques. – La directive NIS 2 est d'une importance capitale, car les changements attendus pour le monde économique sont significatifs dans toute l'Union européenne, mais plus particulièrement en France. En matière de périmètre, le nombre d'entités régulées passe de 500 à 15 000 et le nombre de secteurs économiques concernés passe de 6 à 18 par rapport au cadre de régulation de NIS 1. Cela concerne désormais tous les systèmes d'information des entités régulées et représente un changement majeur de paradigme. Il ne s'agit plus seulement de sécuriser les infrastructures critiques, mais d'assurer la résilience des entités critiques en tant qu'organisation – la couverture est beaucoup plus large.

Je me réjouis de pouvoir entendre vos avis, car vos organisations ont toutes animé des rencontres autour de la transposition de la directive NIS 2 et publié de la documentation générale ou technique à l'attention de vos membres et du grand public. Depuis plus d'un mois, nous menons des auditions auprès de différents représentants sectoriels et j'ai constaté l'ampleur du chemin qu'il reste à parcourir pour une plus grande prise de conscience collective.

Pensez-vous que les entreprises que vous représentez sont suffisamment informées des changements à venir, en particulier le fait qu'elles devront elles-mêmes évaluer si elles entrent dans le champ d'application de la directive, et le cas échéant s'enregistrer auprès de l'Anssi et lui notifier les incidents de cybersécurité ?

Sur la procédure de notification des incidents, la directive NIS 2 prévoit la transmission « sans retard injustifié » d'une alerte précoce dans un délai de 24 heures, puis la transmission d'une notification d'incident dans un délai de 72 heures. Le projet de loi, lui, ne mentionne pas ce double délai. Il contraint les entités à notifier leurs incidents sans délai et évoque la notification d'incidents « critiques » plutôt que d'incidents « importants ». Qu'en pensez-vous ? Sont-ils de nature à surtransposer ou sous-transposer la directive ? Et surtout, sont-ils de nature à affaiblir ou à renforcer notre réponse collective aux cybermenaces ?

Enfin, le Gouvernement a fait des choix sur le périmètre retenu, qu'il nous faut examiner de près. L'inclusion des établissements d'enseignement menant des activités de recherche, des collectivités territoriales, notamment les départements, les métropoles, les communautés urbaines, les communautés d'agglomération et les communes de plus de 30 000 habitants, et l'élargissement du périmètre des entreprises concernées sont autant d'éléments à prendre en compte. Les critères de taille et de chiffre d'affaires sont fixés alternativement, alors que les textes européens les fixent cumulativement. Ces choix sont-ils partagés par les autres États membres ?

Le régime de contrôle et les sanctions prévues sont perçus comme trop punitifs et insuffisamment préventifs. Les acteurs économiques s'inquiètent du coût financier des contrôles réalisés par l'Anssi, qui seraient à leur charge. Je m'interroge sur l'absence de prise en compte du caractère intentionnel de la non-transmission d'informations à l'Anssi, la possibilité d'engager la responsabilité des dirigeants d'entreprise et la rupture d'égalité induite par l'absence de sanctions prévues pour les administrations de l'État. Qu'en pensez-vous ?

M. Hugues Saury, rapporteur pour la commission des affaires étrangères. – Merci pour la clarté de vos propos, dans ce domaine complexe où le jargon prend souvent le dessus : la simplicité est une qualité.

Quels enseignements tirez-vous de la mise en œuvre de la directive NIS 1 et de sa transposition en droit français, qui inciteraient à amender le texte du Gouvernement pour transposer NIS 2 ?

Sauf exception pour la défense, le Gouvernement a choisi de confier à une autorité unique, l'Anssi, la mise en œuvre de la politique gouvernementale en matière de sécurité des systèmes d'information, alors que ce choix n'était pas imposé par la directive NIS 2 : ce choix vous semble-t-il pertinent ?

L'article 6 du projet de loi ne reprend pas les définitions d'incident figurant dans la directive NIS 2, précisées par la suite par un règlement d'exécution du 17 octobre 2024. Cette absence vous semble-t-elle poser des difficultés d'application ? Les définitions retenues par le Gouvernement vous semblent-elles opérantes et suffisamment claires ?

M. Daniel Le Coguic. – Je me focaliserai sur le budget et les éléments de politique industrielle.

Il y a, d'abord, le budget des opérateurs étatiques, en charge de suivre la mise en place du programme ; ce sera à l'État d'en décider, en particulier si c'est l'Anssi qui en est chargée. La dépense à prévoir porte sur plusieurs années, il faut doter les opérateurs en conséquence, donc de crédits pluriannuels. L'application de NIS 1 et la séquence des JO nous montrent qu'il faut trois composantes au budget, trois lignes budgétaires : une pour la sensibilisation, la formation, la communication, sachant que les actions à conduire varient en fonction des priorités, des cibles, des territoires ; il faut une impulsion, sachant qu'il y aura des relais institutionnels, par les organisations professionnelles, les collectivités locales et l'industrie ; deuxième ligne budgétaire, des crédits pour les diagnostics : il faut aider les cibles à connaître leur vulnérabilité, on l'a vu dans les JO pour les stades, cette action doit inclure de la remédiation ; enfin, la troisième ligne budgétaire doit aller à des expérimentations technologiques, pour la mise en œuvre elle-même.

Il faudrait que ces trois lignes budgétaires soient centralisées, comme cela a été fait pour les JO – le plan d'expérimentation cofinancé par l'État et les industriels a donné des résultats importants, il faut poursuivre dans ce sens : 80 % des solutions expérimentées étaient françaises et plus de 96 % européennes, 77 % venaient de PME et de start-up, cela démontre qu'on peut répondre au défi tout en soutenant l'effort d'innovation européen et français.

Nous proposons, ensuite, de soutenir fortement les efforts des entreprises pour la cybersécurité, en mettant en place l'équivalent d'un crédit d'impôt recherche (CIR) pour les inciter à appliquer les nouvelles règles et alléger leur effort financier.

M. Benjamin Leroux. – Les entreprises qui doivent se mettre en conformité sont-elles assez informées ? Celles qui font déjà de la cybersécurité, oui, mais celles qui ne se sentent pas concernées, à tort, vont devoir s'y plonger et elles auront beaucoup de travail – et c'est pourquoi il faut plus de communication.

En matière de régulation et de *reporting*, il est important de savoir vers qui se tourner, des retours d'expérience montrent que l'ensemble est flou et que les entreprises ne savent pas bien à qui s'adresser – d'où le sujet du guichet unique, du formalisme, c'est concret.

Oui, il faut avoir les définitions les plus claires possibles, dans le texte, pour savoir ce qu'est un incident et ce qu'il faut faire selon le type d'incident qui se produit, à qui s'adresser et dans quel calendrier précis – le facteur temps est décisif dans la crise cyber, le formalisme ne doit pas ralentir l'action, il faut aller vite pour redémarrer les systèmes et limiter les pertes : la notification et le partage d'informations sont importants, mais il ne faut pas les privilégier au détriment de la réactivité.

Deux autres enseignements de la directive NIS 1. Le volet cyber des différentes versions de la loi de programmation militaire (LPM) a initié une dynamique pour les structures concernées, avec des réflexes tels que l'homologation, l'audit et le contrôle. En revanche, NIS 1 n'a pas eu un effet aussi important, car des structures se sentaient beaucoup moins concernées. La question de la sanction, qui reste un élément structurant en particulier pour les entreprises, sera utile pour inciter à se protéger.

Enfin, le choix de l'Anssi comme autorité unique nous semble pertinent. L'Agence a fait un travail de fond pour se rendre visible, elle est reconnue pour son accompagnement et, même si elle doit désormais s'adapter pour parler à plus de structures, la dynamique initiée est intéressante à poursuivre.

M. Sebastien Garnault. – Avons-nous eu des informations pour les acteurs financiers, via l'ACPR ou la Banque de France ? Non, mais nous sommes proches de Paris Europlace, qui a un nouveau président de sa commission cyber, c'est par ce canal que nous coopérons avec les institutions financières.

Sur l'écosystème européen, il n'est pas toujours facile de donner une nationalité à une entreprise : est-ce qu'Air France est française, quand 49 % de ses parts sont détenues par les Pays-Bas ? En réalité, on peut faire de la souveraineté avec de l'argent étranger, voyez le projet américain *Stargate*, financé par le Japon, et je crois que le plus important, c'est de connecter nos industries nationales avec l'activité, les projets. Si on veut faire un marché unique, il faut connaître nos collègues, et c'est ce que nous faisons en développant nos relations avec les agences européennes et nos collègues du secteur privé.

L'articulation entre Dora et NIS 2 ne va pas de soi, c'est un euphémisme. En réalité, beaucoup de gens ne sont pas suffisamment informés, – ils s'informent comme ils le peuvent –, et c'est aussi pourquoi il y a ici une responsabilité politique : le jour où un ministre prendra le sujet à bras-le-corps et définira une stratégie claire et dotée de moyens, le sujet aura véritablement de la visibilité. Cela aiderait beaucoup que l'impulsion vienne du plus haut niveau, on l'a vu pendant la crise sanitaire avec l'application StopAntiCovid, il a suffi d'une annonce du Président de la République pour avoir des millions de téléchargements dans la journée et propulser cet outil qui paraissait ne jamais pouvoir décoller… Le sujet est interministériel, c'est pourquoi nous aurions aimé qu'un ministre délégué auprès du Premier ministre en soit chargé.

Les délais sont intéressants, car il y a une « mise en défaut par défaut » qui permettra à l'Anssi de perquisitionner si vous n'avez pas respecté les délais, donc d'avoir un accès direct – cependant, en tant que chef d'entreprise, cela me questionne sur le secret des affaires.

Un problème, me semble-t-il, vis-à-vis des collectivités territoriales : ce projet de loi exonère les communes de moins de 30 000 habitants, alors qu'elles sont souvent les premières victimes et les plus faibles. Je crois qu'il vaut mieux les couvrir aussi contre le risque cyber, et miser sur une montée en compétence des élus. Je suis à votre disposition pour mettre le sujet au cœur du prochain Congrès des maires, c'est un sujet dont il faut parler clairement, d'autant que cela va coûter de l'argent.

L'autorité chargée de la mise en place, ensuite. En général, quand on est un régulateur et qu'on sanctionne, on est une autorité administrative indépendante. L'Anssi est très concrètement à nos côtés, elle nous accompagne, ce serait dommage qu'elle se retrouve dans la position de la CNIL, qui ne va pas sans défiance…

Oui, REC s'articule avec NIS 2, mais nous ne sommes pas les mieux placés pour en parler, vous aurez plus d'éléments dans vos auditions des semaines à venir.

Mme Anne Elise Jolicart, membre de CyberTaskForce. – Une précision sur les enseignements à tirer de l'application de la directive NIS 1. Elle visait à renforcer la résilience, on a vu alors qu'il y avait des trous dans la raquette ; la bonne nouvelle, c'est que NIS 2 veut les combler, en changeant de paradigme, avec un nouveau périmètre et une définition des vulnérabilités qui couvre les aspects techniques, mais aussi le facteur humain. La directive est claire sur ce point, et nos voisins allemands, italiens et belges l'ont précisément transcrite, y compris, pour les Allemands, en chiffrant le rançongiciel par exemple, c'est une avancée pour renforcer la résilience.

La question des définitions est fondamentale. Albert Einstein disait que s'il avait une heure pour sauver le monde, il passerait 55 minutes à définir le problème et 5 minutes pour le résoudre. Si on ne définit pas bien le problème, je ne vois pas comment on pourra atteindre les objectifs de la directive. Le Conseil d'État a rappelé l'importance des définitions, y compris si cela implique d'ajouter des définitions qui ne sont pas dans le texte originel. C'est ce qu'ont fait les Allemands et les Italiens quand ils ont repris la définition d'approche tous risques qui inclut expressément le risque lié au facteur humain.

M. Christian Daviot. – Il n'y a pas eu d'évaluation sérieuse de NIS 1 – celle qui a été faite à l'échelon européen n'a été lue par personne, ce qui vaut peut-être mieux... En France, nous avons surtransposé NIS 1, en ajoutant 9 secteurs d'activité.

Un élément qui nous différencie peut-être dans cette table ronde : nous pensons que, pour les collectivités territoriales, l'échelon régional est le bon, et qu'il ne faut pas descendre jusqu'aux communes, sauf peut-être à relever le seuil démographique, par exemple à 80 000 habitants. La directive mentionne l'échelon régional, il nous parait le meilleur, il y a d'autres façons

de couvrir les communes qu'avec les obligations et sanctions prévues par NIS 2, qui peuvent passer par la voie réglementaire.

Enfin, sur le pilotage, nous pensons que la question est moins celle de l'autorité unique que celle de l'efficacité du dispositif d'ensemble, qu'il faut évaluer. France 2030 a engagé environ 750 millions d'euros sur la cybersécurité, cet argent a-t-il été dépensé efficacement, quels sont les enseignements d'organisation ? Nous avons besoin d'une évaluation globale du dispositif national de cybersécurité. Il faudrait s'appuyer sur des structures existantes pour aider à mettre en œuvre une stratégie d'ensemble, mais l'Anssi ne peut pas tout faire, en particulier en région.

M. Farid Lahlou, membre de l'Alliance pour la confiance numérique. – J'ai co-fondé la société BonjourCyber, qui développe un outil ciblé sur la protection des PME et des ETI. Quand une entreprise se demande comment se déclarer, une grande partie du chemin est déjà fait ; la vraie difficulté, c'est de concerner les entreprises qui ne connaissent pas du tout le danger, ni les parades. Les entreprises recherchent avant tout un retour sur investissement, elles se focalisent sur leur trésorerie et leur chiffre d'affaires, il est difficile de les intéresser d'emblée à une menace qu'elles ne perçoivent pas.

L'initiative des chèques cyber de la région Île-de-France montre, me semble-t-il, que la communication n'est pas qu'institutionnelle, elle gagnerait à être aussi commerciale : les entreprises de cybersécurité jouent un rôle clé dans l'identification des entreprises soumises à NIS 2, nous n'avons pas suffisamment souligné leur rôle.

Enfin, on demande aux entreprises de se déclarer dans des délais raisonnables et l'on parle de sanctionner celles qui ne l'auront pas fait ; prises par leurs problèmes de trésorerie, leur focus sur le chiffre d'affaires, les entreprises risquent fort de reporter leur déclaration, donc des sanctions par la suite ; puisque le mécanisme de sanction n'est pas prêt d'être en place, est-ce qu'une incitation serait possible entretemps, pour accélérer le mouvement ?

M. Ludovic Haye. – Merci pour ces propos complets et complémentaires les uns des autres. Quand un élu local me dit que la loi est mal faite, je réponds qu'il est difficile de faire des normes qui vaillent aussi bien pour une métropole de plus de 100 000 habitants, que pour un village de 50 habitants. Ce qu'il faut, c'est une bonne articulation sur le dernier kilomètre, c'est là où nous avons notre rôle, cela vaut aussi pour la cybersécurité et l'application de NIS 2. L'écart est énorme entre une entreprise du CAC 40, qui dispose d'une direction des services informatiques importante, et une commune qui a pour toute ressource technique une secrétaire de mairie à temps partiel… Il y a un sujet de bon sens, de système D, qui ne coûte pas cher, mais qui a son importance. Lorsque je visite des communes, je demande si les services ont au moins une sauvegarde – la plupart du temps, la réponse est floue, me confirmant qu'un plan de reprise d'activité n'a pas été fait et qu'on n'est pas en mesure, le jour de l'attaque, de

repartir. La directive NIS 2 ne doit pas être une épée de Damoclès supplémentaire pour les communes, une menace supplémentaire d'amende administrative : ce n'est pas la sanction qui va résoudre le problème des communes, il faut les accompagner dans le dernier kilomètre.

Enfin, j'alerte sur le caractère opportuniste de certaines entreprises sur le marché de la cybersécurité, qui prétendent avoir les solutions pour parer à tout : les maires et les adjoints ont besoin d'accompagnement pour séparer le bon grain de l'ivraie.

Mme Catherine Morin-Desailly. – Vous avez parlé des conditions normales de la commande publique comme levier de développement pour nos entreprises françaises et européennes. Qu'entendez-vous par conditions normales, alors que nombre d'entreprises européennes dénoncent des rédactions biaisées dans les appels d'offres, qui favorisent les entreprises extra-européennes ? C'est ce qui s'est passé avec la plateforme des données de santé.

La Direction interministérielle du numérique (Dinum) a-t-elle des directives précises sur ce point ? La Cour des comptes travaille actuellement sur ce sujet, qui répond à la question pertinente de M. Canévet : avons-nous les moyens de développer un écosystème numérique et de récupérer progressivement des briques de souveraineté ?

Mme Michelle Gréaume. – La cybersécurité en entreprise, comme celle des petites collectivités territoriales, est d'autant plus menacée que la vulnérabilité a augmenté avec le développement du télétravail, lui-même lié à la crise sanitaire. Les TPE et les PME sont logiquement les premières cibles des criminels, alors qu'elles ont moins de moyens pour se protéger. Dès lors, comment rendre plus attractifs les investissements en cybersécurité, en faire un atout économique de protection des salariés, de l'activité et une opportunité pour les entreprises de votre secteur ?

Concernant la commande publique, quels freins rencontrent aujourd'hui les entreprises du secteur pour gagner des marchés publics, en dehors des parts de marché importantes des États-Unis ?

La manipulation des élections en Europe, notamment l'annulation d'un scrutin présidentiel en Roumanie en raison de la diffusion de fausses informations et de manipulations numériques d'ampleur, pose question. La situation a donné lieu à une passe d'armes entre Elon Musk et Thierry Breton. Dans quelle mesure la protection des systèmes électoraux constitue-t-elle un enjeu pour les entreprises de votre secteur, alors que les élections législatives allemandes sont menacées par la manipulation et la désinformation ?

Enfin, la panne informatique mondiale de juillet 2024 a montré la fragilité du système numérique global, notamment pour les entreprises utilisant les logiciels de Microsoft avec *CrowdStrike*. Comment analyser cette panne et l'évolution de la cybersécurité en France ?

M. Olivier Cadic, président. – Je propose, surtout vu le temps imparti, de laisser de côté les questions concernant la manipulation de l'information, car ce sujet n'entre pas exactement dans notre sujet.

Mme Audrey Linkenheld. – À Lille, nous avons subi une cyberattaque d'ampleur, alors que j'étais première adjointe de Martine Aubry, et cette expérience me fait souligner qu'en matière de cybersécurité, comme vous le dites, le problème et la solution résident aussi bien dans les gens que dans les systèmes – donc pas seulement dans les systèmes informatiques.

La différence entre les collectivités et les entreprises, c'est que si les entreprises voient un impact financier immédiat aux menaces cyber, ce n'est pas tout à fait aussi vrai pour les collectivités. L'enjeu pour elles n'est pas tant financier que dans la continuité des services publics et dans la question du process plus général, qui n'est pas toujours informatique. Il faut examiner cet aspect des choses et répondre à cette question : si le système informatique fait défaut, comment rend-t-on quand même le service public ? Ce n'est pas qu'une question d'argent, il faut un accompagnement, pour anticiper les choses et connaitre nos vulnérabilités.

Enfin, que pensez-vous des *computer security incident response team* (CSIRT) mis en place à l'échelon régional avec du soutien public ?

M. Stéphane Meynet, membre du CyberCercle. – Les entreprises sont préoccupées par la conformité aux normes internationales ou sectorielles, ce qui leur permet d'avoir des parts de marché supplémentaires ou de ne pas en perdre, plutôt que de se conformer à une réglementation sur la cybersécurité, il faut prendre en compte cette réalité.

La mise en place d'un nouveau texte oblige les entreprises à démontrer leur conformité à des normes et à des réglementations, ce qui représente un double travail. Ne peut-on pas harmoniser les réglementations pour simplifier le travail des entreprises et des collectivités territoriales ? Il serait utile de dresser un état des lieux de ce qui existe avant de proposer un texte supplémentaire…

M. Daniel Le Coguic. – Cette transposition donne l'occasion de mettre en mouvement la filière de la cybersécurité, au service des territoires, des organisations publiques et des entreprises – et mon message est simple : il faut être ensemble, anticiper, innover et collaborer. C'est le point clé, beaucoup de cibles sont manquées, il faut simplifier le chemin de la mise en conformité avec des solutions technologiques.

Nous avons aussi besoin d'un programme de filière, avec une dimension de service et une dimension d'expertise, nous manquons de ressources humaines et d'outils technologiques. Il faudra peut-être faire un effort de certification, de labellisation des entreprises qui seront « NIS 2 compatibles », à nous de proposer une forme d'habilitation, de labellisation, ceci pour simplifier les décisions des collectivités, des hôpitaux, des entreprises. La commande publique a son rôle à jouer, évidemment. Il ne s'agit

pas de suréquiper les collectivités, mais de définir des solutions adaptées aux besoins. L'industrie doit avoir une vision de prédiction sur le long terme pour proposer une économie générale intéressante. Il faudra s'inspirer de ce que fait la Direction générale de l'armement (DGA) ou l'armée dans le cadre de la LPM. Cela donnera la visibilité aux industriels dans le cadre d'un programme sur plusieurs exercices.

M. Benjamin Leroux. – Il faut apprendre de nos expériences pour éviter de répéter les erreurs du passé, notamment celles du RGPD – tout le monde disait alors avoir une solution miracle, mais les problèmes ont persisté…

La certification et la labellisation sont des sujets importants. Il y a des solutions, mais il faut les adapter pour être à la bonne échelle ; les visas de sécurité de l'Anssi peuvent être une solution, à vérifier – il faut s'inspirer de l'existant pour éviter des coûts supplémentaires pour les sociétés de cybersécurité, la labellisation coûte cher, alors qu'il faut être opérationnel rapidement. Il faudrait peut-être un label d'échelon européen, pour faire le tri entre les professionnels européens les plus adaptés et les opportunistes, mais aussi conforter les acteurs les plus compétitifs.

Oui, le facteur humain, l'organisation sont décisifs, au-delà de la technologie. La cybersécurité a besoin de sensibilisation et de préparation. Il faut prévoir le pire et savoir comment gérer une crise. Cela doit faire partie de l'accompagnement, car pendant la crise, il faut poursuivre les activités, que ce soit pour une entreprise ou une administration.

La panne informatique de juillet 2024, liée au logiciel *CrowdStrike*, nous alerte sur le risque avec les solutions d'accès distant, des pare-feu ont fait l'objet de vulnérabilités. L'Anssi s'en est inquiétée, il est malheureux que des briques de cybersécurité… posent des problèmes de cybersécurité. Le *Cyber Resilience Act* devrait responsabiliser ceux qui fabriquent des objets numériques, pour qu'ils y mettent un peu plus de protection par défaut.

Mme Anne Elise Jolicart, membre de CyberTaskForce. – Nous avons travaillé sur les vulnérabilités humaines, et précisé les choses dans des fiches, que nous pourrons vous transmettre.

Un mot sur la question de la lutte contre la manipulation de l'information, un domaine que je connais bien, en tant que membre de groupes de travail du CNRS sur le sujet et réserviste opérationnelle pour l'armée. Lutter contre les vulnérabilités humaines et maitriser l'empreinte numérique des citoyens, cela revient précisément à traiter cette menace, les sujets sont très liés.

M. Philippe Luc. – Des actionnaires et des administrateurs d'entreprises cotées, par exemple, peuvent être influencés ou contraints, voire déstabilisés par des actions d'origine cyber. Et il faut bien voir que dans les élections pour le Brexit ou la première élection de Donald Trump, le piratage n'a pas porté sur les systèmes électoraux, mais sur les cerveaux des électeurs.

C'est tout à fait comparable pour les actionnaires et les responsables d'entreprise, ils sont des cibles pour les menaces cyber.

M. Olivier Cadic. – Je suis tout à fait d'accord. Viginum a publié un rapport pour prévenir les entreprises des menaces de divers ordres, qui peuvent avoir un impact sur le cours de la Bourse. Cependant, ces aspects ne font pas partie de ce projet de loi de transposition. Mais si vous pensez qu'il faut ajouter des articles pour trouver des moyens de lutter contre la désinformation, vous pouvez compter sur moi – même si je ne vois pas bien comment la loi pourrait empêcher, par exemple, que de grandes personnalités reprennent les éléments de langage de pays étrangers sur nos propres chaînes de télévision... Le sujet est donc ô combien intéressant, mais il n'est pas dans le texte auquel nous devons nous tenir.

M. Sébastien Garnault. – Nous sommes d'accord avec l'idée qu'en dessous de 30 000 habitants, par exemple, il vaille mieux passer par les intercommunalités que s'adresser aux communes, il faut rechercher la solution la plus efficace.

Sur la lutte contre la manipulation informationnelle, des coopérations existent entre pays européens ; après l'annulation de l'élection présidentielle en Roumaine, le directeur de l'Anssi roumaine nous a transmis des documents aussitôt qu'ils avaient été déclassifiés – la coopération n'est pas institutionnalisée mais elle existe, entre personnes, même s'il ne faut pas oublier que sur des sujets aussi sensibles, l'intérêt national prime rapidement. Les Américains, il faut le dire aussi, savent très bien exploiter le marché de la menace cyber.

Enfin, s'agissant des CSIRT régionaux, je ne peux que vous transmettre ce qu'on m'en dit, car je n'en ai pas d'expérience directe. On me dit qu'il y a un problème de fond, et de forme. Il y aurait une perte d'information. Et leur financement par l'État ne semble pas pérenne, sans que les régions paraissent devoir prendre le relais – pour ce que j'en sais, ce n'est pas très positif.

M. Christian Daviot. – Attention, les CISRT régionaux ne sont pas de véritable CSIRT, il faudrait arrêter de les désigner par ce terme. Cette appellation est normalisée et obéit à des règles ; or, les personnes travaillant actuellement dans ces structures régionales n'assument pas les missions qui sont censées être celles d'un CISRT.

M. François Coupez, membre du CyberCercle. – L'aspect humain est pris en compte dans la directive NIS 2. L'article 20 sur la gouvernance prévoit des formations pour les dirigeants et une sensibilisation des personnels. Ces éléments viendront a priori dans les textes réglementaires en application de la loi, avec des obligations de formation spécifiques pour les acteurs du numérique, qui sont déjà couverts par le règlement d'exécution du 17 octobre 2024 – nous pourrons vous en détailler le contenu par écrit, il y a tout un

ensemble de mesures, un encadrement avec les chartes d'utilisation des moyens de système informatique, et des sanctions.

Les règles prévues par Dora et NIS 2 sont articulées, puisque dès qu'un établissement – du secteur bancaire, financier ou assurantiel – respecte Dora, il est conforme à NIS 2. Des questions se posent sur les procédures de notification, pour éviter les doublons ou les lourdeurs ; l'ACPR et l'Anssi se concertent actuellement pour faire au mieux, il faut s'assurer que les règles nouvelles n'alourdissent pas les procédures. Dora prévoit des règles plus fortes, qui de ce fait satisfont NIS 2. Mais il faut bien voir que le mouvement va se prolonger, il y aura une directive NIS 3, qui sera un mix entre les deux – quelque chose comme une directive « Doris » –, avec un contrôle jusqu'au dernier sous-prestataire, que l'on trouve dans la résilience opérationnelle de Dora. La directive NIS 2 comprend une clause de revoyure, comme le faisait NIS 1, et l'on sait que vers la mi-2027, on va se poser la question du prochain texte, qui entrera en vigueur mi-2028.

Les contraintes ne portent pas uniquement sur les entités essentielles, elles vont être sur leurs sous-traitants, à travers des audits très précis sur l'activité des sous-traitants. Il va se passer la même chose qu'il y a vingt ans avec le Règlement 97/02 sur les établissements financiers, les prestataires vont devoir s'adapter pour devenir sous-traitants d'opérateurs couverts par NIS 2, cela va tripler voire quadrupler le nombre d'acteurs couverts par ces règles.

M. Olivier Cadic, président. – Merci pour toutes ces informations. Je reprendrai les mots de Daniel Le Coguic : il nous faut être ensemble, collaborer. Si nous avions été ensemble et si nous avions collaboré, il n'y aurait peut-être pas eu besoin des CSIRT régionaux et l'argent public aurait été dépensé autrement. Nous devons donc travailler ensemble, et avant de dépenser de l'argent public, commençons par nous interroger sur les objectifs – il est toujours trop confortable de se dire qu'en mettant plus d'argent sur la table, on règle les problèmes…

Sous réserve de l'approbation de la conférence des présidents, nous pourrions examiner ce projet de loi le 11 mars prochain. Je vous invite à nous faire parvenir par écrit vos analyses et vos propositions d'amendements, nous les partagerons avec tous les rapporteurs.

Je souhaite une transposition intelligente de NIS 2, c'est-à-dire faite par les professionnels, pour les professionnels. Chacune de vos propositions sera partagée entre vous tous, nous ne vous dirons pas nécessairement d'où ces propositions viennent, mais nous vous demanderons votre avis – nous voulons que nos ajouts, finalement, aient été passés au crible de la critique et qu'ils aient été élaborés de façon collective. On ne peut plus légiférer sans consulter ni même sans associer ceux qui seront chargés de l'application des normes : c'est une démarche nouvelle, nous voulons la conduire dans la transparence. Vous êtes les professionnels qui aurez en charge d'aider les entreprises à se mettre en conformité, il est donc essentiel que vous puissiez

également examiner ce texte et y contribuer à votre niveau – je souhaite que ce travail soit interactif. Merci encore pour votre apport, il est essentiel.

LUNDI 27 JANVIER 2025

Audition de Mme Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique

M. Olivier Cadic, président. – Madame la ministre, notre commission spéciale s'est constituée le 12 novembre dernier, et nous devions ouvrir notre cycle d'auditions par votre audition le 9 décembre, date que nous avions prévue avant que la censure n'entraîne la démission du précédent gouvernement. Après une si longue attente, nous vous remercions et nous réjouissons de votre présence ce matin, signe d'une continuité ministérielle bienvenue pour le suivi d'un texte très attendu par les professionnels de la cybersécurité et tous les utilisateurs de systèmes d'information, c'est-à-dire tout le monde !

En effet, ce projet de loi vise la transposition de trois directives différentes : la directive (UE) 2022/2557 sur la résilience des entités critiques, dite « REC » ; la directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS 2 » ; et la directive (UE) 2022/2556 qui concerne la résilience opérationnelle numérique du secteur financier, dite « Dora ».

Votre présence est aussi le signe qu'enfin le calendrier se dégage pour l'examen de ce texte en séance au Sénat, qui devrait intervenir le 11 mars prochain, sous réserve de confirmation dans les prochains jours par la conférence des présidents.

Avant de vous accueillir, la commission spéciale n'est pas restée inactive. Les rapporteurs ont mené des auditions et nous nous sommes rendus à Bruxelles auprès de la Commission européenne et des autorités belges qui ont d'ores et déjà transposé la directive NIS 2 selon un modèle intéressant faisant notamment référence à la norme ISO 27001. La commission a également entendu M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), et organisé deux tables rondes réunissant, d'une part avec le Mouvement des entreprises de France (Medef) et la Confédération des petites et moyennes entreprises (CPME), d'autre part avec des associations d'experts de la cybersécurité : l'Alliance pour la confiance numérique (ACN), le Clusif, le Cyber Cercle et la Cyber Task Force.

Ces auditions ont d'ores et déjà soulevé un certain nombre de préoccupations sur l'économie du projet de loi, le rôle de l'Anssi, les obligations et sanctions applicables aux entreprises.

La transposition de ces directives est essentielle pour renforcer la cybersécurité en Europe, mais le projet de loi présente des risques de divergences par rapport aux autres pays européens. D'après les premières auditions, il apparaît crucial d'adopter une approche proportionnée en évitant les surtranspositions et en harmonisant les obligations de sécurité.

Madame la ministre, avant de vous donner la parole, je rappelle que cette audition fait l'objet d'une captation vidéo qui est retransmise sur le site internet du Sénat, puis consultable en vidéo à la demande.

Mme Clara Chappaz, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargée de l'intelligence artificielle et du numérique. – Permettez-moi de vous remercier pour cette audition, dont l'organisation a en effet été bousculée par l'actualité politique des dernières semaines. C'est un honneur de pouvoir m'adresser à vous sur le renforcement de la cybersécurité et la résilience de nos infrastructures numériques, un sujet d'intérêt stratégique qui n'est plus réservé à des experts techniques.

Nous sommes confrontés à des menaces multiples et toujours plus nombreuses tant dans le monde physique que dans l'environnement numérique. Aux risques naturels, sécuritaires et sanitaires s'ajoutent des risques technologiques et des menaces liées à des ingérences étrangères. La crise sanitaire du covid-19 a souligné combien l'économie mondialisée reposait sur des chaînes de valeurs diffuses et des processus de production extrêmement fragmentés, de la conception à la distribution.

Toute perturbation de nos services essentiels, même initialement limitée à une entité ou un seul secteur, peut produire des effets en cascade et avoir une incidence négative de grande ampleur sur la fourniture des services au sein du marché européen. Au pic de la pandémie, le retour des contrôles aux frontières a perturbé la poursuite de certaines de nos activités.

Le contexte géopolitique, géoéconomique et sanitaire international se caractérise désormais par une particulière instabilité. Des conflits locaux ont une incidence mondiale, à l'instar de la guerre en Ukraine qui a perturbé l'approvisionnement en céréales, ou encore de la confrontation entre Israël et le Hamas. Les exemples de retard ou de pénurie de produits sont nombreux. Lors de la crise sanitaire, la prise de conscience de ce phénomène s'est accélérée, car la France a constaté sa dépendance par rapport à la production de paracétamol et autres principes actifs. De la même manière, la bascule majeure de notre pays en télétravail a accru notre exposition aux risques cyber.

Dans ce climat, l'utilité de chacun des titres du projet de loi dit « Résilience » est démontrée sans détour.

Le titre I^er^, qui transpose la directive REC, s'attache d'abord à maîtriser la variété des risques auxquels sont confrontés nos infrastructures et opérateurs critiques. Nous ne partons pas de rien. En effet, dès 2006, la France a fait le choix précurseur de mettre en œuvre un dispositif de protection des

secteurs d'activité d'importance vitale. Mais l'évolution vers une plus grande imprévisibilité politique ainsi que la diversification des menaces doit conduire les opérateurs concernés à prendre en compte la sécurité non plus seulement de leurs installations physiques, mais de tous les éléments qui concourent au fonctionnement de leur activité.

En outre, la cybersécurité est désormais un pilier de notre souveraineté, une composante de notre robustesse économique et financière, et un préalable à la confiance que placent nos concitoyens dans les services numériques – vous l'avez dit, chacun d'entre nous en bénéficie. Une prise de conscience collective s'impose à nous au gré de la multiplication des incidents à tous les échelons.

C'est à cette question que s'attache à répondre le titre II du projet de loi consacré à la directive NIS 2. Là aussi, nous ne partons pas de rien : la France disposait dès 2013 d'une réglementation robuste pour renforcer la cybersécurité des systèmes d'information d'importance vitale. Ce cadre a été complété avec la directive NIS 1, au profit de près de 300 opérateurs de services essentiels (OSE) qui étaient la cible privilégiée d'une menace cyber dite « stratégique ». Ces OSE ont gagné en maturité dans la gestion de leurs menaces en ligne, ont intégré la réglementation dans leurs procédures internes et ont ainsi évolué avec succès vers des systèmes d'information plus robustes.

Cependant, comme le directeur général de l'Anssi l'a mentionné, la menace cyber a fortement évolué ces dernières années. Historiquement très stratégique, elle est devenue systémique et émane de plus en plus de groupes cybercriminels organisés, qui opèrent à but lucratif ou s'efforcent de nous déstabiliser pour des raisons idéologiques. Les attaques par rançongiciel, *phishing* ou d'origine étatique ciblent non plus uniquement les grandes entreprises ou les infrastructures critiques, mais bien l'ensemble du tissu économique et social. Elles ont augmenté de 30 %, et 60 % d'entre elles visent les TPE-PME et les collectivités territoriales – certaines ne font l'objet d'aucune réglementation cyber ; parallèlement, la maturité des entités essentielles rend les nouvelles entités beaucoup plus attractives aux yeux des cybercriminels.

À titre d'exemples, je citerai l'attaque perpétrée au mois d'octobre contre le groupe Hospi Grand Ouest, qui a entraîné la déprogrammation de plusieurs opérations, ou celle qui a visé le centre hospitalier de Bourg-en-Bresse. Une étude menée par trois chercheuses de l'université du Minnesota a d'ailleurs démontré que, en cas d'intrusion par rançongiciel, la mortalité des patients déjà admis à l'hôpital augmentait sensiblement. Les collectivités territoriales ne sont pas en reste ; elles sont même une cible privilégiée. Entre janvier 2022 et juin 2023, l'Anssi a traité en moyenne dix attaques par mois contre une collectivité.

Face à l'évolution de la menace et à l'ampleur de ses conséquences, les États membres de l'Union européenne, dont la France, ont jugé qu'il était impératif de moderniser le cadre réglementaire et se sont mobilisés en ce sens.

Ces efforts concernent également le système financier, tout aussi exposé, plus de la moitié des banques ayant été victimes d'une attaque réussie en 2024, selon les chiffres de l'Autorité bancaire européenne (ABE). Cette même année, les sites de La Poste et du Crédit Agricole étaient piratés, avant que la Banque de France confirme pour sa part avoir constaté des intrusions sur l'un de ses extranets. La transposition de la directive accompagnant le règlement Dora au sein du titre III du présent projet de loi nous permettra donc d'identifier les risques cyber spécifiques qui pèsent sur ce secteur.

Les exemples concrets que j'ai cités illustrent combien certaines menaces ont des répercussions tangibles sur le quotidien de nos entreprises, de nos collectivités et, surtout, de nos concitoyens. Ces attaques ont un coût très élevé, estimé en 2022 par le cabinet d'études économiques Asterès à 2 milliards d'euros, et contribuent à ébranler la confiance qu'ont les Français dans la capacité de nos institutions publiques à les protéger.

Le présent projet de loi envisage une démarche globale qui s'exprimera *ex ante* par une meilleure prévention des risques, et *ex post* par une réaction rapide et efficace en cas d'incident. À ce titre, je tiens à saluer le choix qu'a fait le Sénat de constituer cette commission spéciale, qui permettra de s'appuyer sur l'expertise des commissions des affaires étrangères et de la défense, des finances et des affaires économiques.

J'apporterai maintenant quelques précisions sur chacun des trois volets du texte.

Le titre I^{er}, qui transpose la directive REC, consacre avant tout un changement d'approche quant à la protection des opérateurs fournissant des services vitaux pour les fonctions sociétales ou les activités économiques. Là où le dispositif précédent de sécurité des activités d'importance vitale (SAIV) était concentré sur la protection physique des infrastructures, il s'agit de mettre aussi l'accent sur la résilience et l'adaptabilité des opérateurs nationaux face aux crises, y compris à l'échelle européenne. C'est un cheminement salutaire pour tirer les conséquences des crises passées, tenir compte des interdépendances d'aujourd'hui et mieux protéger demain des activités indispensables à notre vie économique et sociale. Je pense à la santé, à l'alimentation ou à l'eau potable, dont nous avons pu tristement mesurer l'importance pour notre souveraineté au cours des dernières années.

Avec le dispositif de SAIV, environ 300 opérateurs et 1 500 points d'importance vitale faisaient l'objet d'une protection spécifique. La transposition de la directive REC modernisera ce cadre et le rendra plus adapté aux défis actuels. Surtout, cette harmonisation de la réglementation mettra l'ensemble des États membres, dont certains ne possédaient pas de dispositif similaire au nôtre, sur un pied d'égalité. Il s'agira ainsi de rétablir une égalité concurrentielle entre nos opérateurs et leurs homologues européens, tout en apportant une meilleure réponse aux risques transfrontaliers et d'interdépendance des chaînes d'approvisionnement.

La transposition proposée vise donc à préserver les principes de la politique de SAIV tout en restant le plus près possible des exigences de la directive REC. Les entités critiques pourront ainsi continuer à s'appuyer sur une pratique et une méthode éprouvée.

Trois nouveaux secteurs seront couverts – assainissement, réseaux de chaleur et hydrogène –, qui viendront s'ajouter aux douze qui existaient déjà. Autre nouveauté : le passage d'une logique de sécurisation des sites à une logique de résilience, axée sur la continuité de l'activité. Les acteurs concernés devront réaliser une analyse des risques dans des plans de résilience, mieux identifier les dépendances qui les lient à leurs prestataires ou d'autres secteurs, et notifier les incidents majeurs qu'ils pourraient constater. Ces mesures garantissent une prise en compte accrue des risques, qu'ils soient physiques ou numériques.

S'agissant des collectivités territoriales, la directive ne les couvre pas en tant que secteur spécifique. Celles qui sont concernées doivent avoir été désignées comme opérateur d'importance vitale ou de services essentiels dans les secteurs qui relèvent de leur compétence : eau, transport ou énergie. En cas de gestion en régie, les changements seront marginaux.

Le titre I^{er} du projet de loi s'inscrit donc dans une politique cohérente et globale en matière de sécurité, en synergie avec les obligations prévues par les directives NIS 2 et Dora. Concrètement, les entités régulées au titre de la directive REC devront respecter les exigences des deux autres dispositifs.

J'en viens au titre II, consacré à la directive NIS 2 qui vise à renforcer la résilience cyber de tous les États membres de l'Union. L'harmonisation des régimes mis en œuvre sera déterminante. C'est pourquoi la transposition proposée est une transcription fidèle du texte européen. De plus, les négociations puis la rédaction de ce texte ont été guidées par la volonté que la directive puisse être appliquée par tous. Le principe de proportionnalité est donc un fil conducteur du projet. Une distinction claire est ainsi établie entre, d'une part, les entités importantes – elles représentent 80 % de la totalité –, et, d'autre part, les entités essentielles, et ce afin de fixer des obligations adaptées au profil de chaque acteur.

Les premières sont pour la plupart des petites structures, qui bénéficieront d'un régime proportionné centré sur les bonnes pratiques d'hygiène numérique, en s'appuyant sur le guide rédigé par l'Anssi. Cette approche permettra de munir les plus fragiles d'un filet de sécurité cyber minimal. Les secondes, dont la majorité est déjà soumise aux réglementations précédentes et absorbera à moindres frais les coûts de conformité associés, devront respecter des contrôles accrus, du fait des risques de conséquences en cascade dans des secteurs connexes, voire dans d'autres pays. Ces acteurs sont déjà bien armés par leur taille, leur surface financière, leur dispositif de gestion des risques et leurs connaissances des enjeux de cybersécurité.

Grâce à un champ d'application large, des exigences proportionnées, adaptées et raisonnables, la transposition de la directive NIS 2 fera de la cybersécurité un élément du socle fondamental de notre Nation, de notre société et de notre économie. Au total, plus de 15 000 entités seront régulées en France, dans 18 secteurs d'activité. Elles devront répondre à différentes exigences : s'enregistrer auprès de l'Anssi ; notifier les incidents ayant un impact important sur la fourniture de leurs services et potentiellement en informer le public ; prendre des mesures adaptées pour protéger leurs réseaux et systèmes d'information.

Si vous y consentez, les objectifs de sécurité seront précisés par voie réglementaire, afin que nous disposions de plus de souplesse pour les faire évoluer. Le référentiel a déjà fait l'objet de plusieurs concertations et continuera d'être coconstruit jusqu'à sa parution.

S'agissant des collectivités territoriales, la directive prévoit un droit d'option que le Gouvernement a choisi d'activer, car plus d'un quart des victimes d'attaques par rançongiciel recensées par l'Anssi en 2023 étaient des collectivités. Elles seront environ 1 800 à relever directement de NIS 2. Celles de moins de 30 000 habitants, c'est-à-dire l'immense majorité des communes, ne seront concernées qu'à travers leur intercommunalité de rattachement.

Nous sommes bien conscients des efforts que certaines collectivités devront accomplir. Sans remettre en cause l'objectif et l'intérêt de ce projet de loi, les associations d'élus locaux ont exprimé un vrai besoin d'accompagnement.

J'en viens enfin au troisième volet du projet de loi, relatif au renforcement de la résilience numérique du secteur financier. Banques en ligne ou mobiles, paiements électroniques : les institutions financières sont toujours plus exposées aux risques cyber. Le système financier est en outre très interconnecté à l'échelle mondiale, ce qui l'expose aux risques de contagion et d'incidents systémiques. Selon le FMI, il aurait subi plus de 20 000 incidents en vingt ans et connu une perte de 28 milliards de dollars pour la seule période 2020-2024.

Jusqu'au règlement Dora, les établissements financiers devaient s'appuyer sur huit directives européennes différentes. Le chevauchement de ces textes et l'hétérogénéité des approches nationales ne permettaient pas un fonctionnement optimal du marché intérieur. L'harmonisation apportée par le règlement Dora est donc la bienvenue. La France l'a négocié en exigeant qu'il soit précisément articulé avec NIS 2, dont il constitue une déclinaison sectorielle. Ce règlement est construit sur cinq piliers principaux : l'adoption de procédures d'identification et d'atténuation des risques liés aux technologies ; la mise en place d'une procédure de notification des incidents ; la réalisation de tests de résilience opérationnelle ; l'encadrement de la gestion des risques liés à leurs prestataires ; enfin, le partage d'informations entre entités financières afin d'améliorer notre résilience collective.

La directive accompagnant le règlement Dora qu'il est proposé de transposer vise à assurer une cohérence juridique et technique entre le règlement, d'application directe, et les huit directives que je viens d'évoquer.

Vous l'aurez compris, le projet de loi Résilience est un texte ambitieux et pragmatique qui repose sur une philosophie claire : protéger efficacement sans entraver l'innovation et la compétitivité. Nous devons donc tenir une ligne de crête que je résumerai en trois principes : proportionnalité, concertation, accompagnement.

Ce texte, qui se fonde sur une approche proportionnée, a été construit au terme d'une large concertation. L'Anssi a ainsi mené plus de 70 consultations depuis septembre 2023 sur la transposition de NIS 2. J'ai moi-même eu l'occasion de m'entretenir dès ma prise de fonction avec des élus, notamment plusieurs d'entre vous, des associations d'élus, des entreprises et des fédérations, partout sur le territoire. Ce dialogue est bien entendu amené à se poursuivre tout au long de la vie du texte, y compris sur son volet réglementaire et pendant sa mise en œuvre.

Enfin, le Gouvernement entend naturellement répondre à la demande consensuelle d'accompagnement qui s'est exprimée. L'objectif de ce texte n'est pas de sanctionner, mais d'identifier nos points de vulnérabilité et de renforcer notre sécurité numérique au bénéfice de tous. Aujourd'hui, la question n'est plus de savoir si une entité sera attaquée, mais plutôt quand elle le sera. J'ai conscience que pour certains acteurs nouvellement assujettis, la marche semble haute, mais rappelons que le coût de la sécurité est cent fois inférieur au coût d'une attaque réussie.

Au-delà des outils en ligne que l'Anssi a développés, et qu'elle enrichira – MonAideCyber, MonEspaceNIS2 –, des réseaux de terrain joueront un rôle de proximité particulièrement précieux pour les entités régulées. Je pense notamment aux chambres de commerce, aux campus cyber régionaux, aux centres de réponse aux incidents de sécurité informatique (CSIRT) et aux fédérations professionnelles qui seront autant de relais utiles dans nos territoires. Nous sommes en train de travailler à un renforcement, une meilleure structuration et une plus grande lisibilité de ces réseaux et guichets de terrain afin que les entités régulées puissent disposer d'un parcours clair, de l'évaluation de sécurité jusqu'à la sollicitation des services de remédiation, en passant par la notification d'incident.

Au final, ce texte constitue une opportunité d'élever collectivement nos compétences et notre conscience en matière de risque cyber, et d'opérer un changement de culture. L'intégration de la gestion des risques cyber dans les stratégies des organisations est désormais impérative. Nous continuerons les efforts de sensibilisation en ce sens et veillerons à ce que l'ensemble des citoyens adoptent les pratiques d'une bonne hygiène numérique.

Je porte aussi la conviction personnelle que le présent projet de loi est une opportunité unique pour notre écosystème cyber français. Dans un

marché de la cybersécurité en pleine expansion, nos entreprises, dont les compétences sont reconnues, ont un rôle clé à jouer à l'échelle européenne. En renforçant la sécurité de nos infrastructures, nous stimulerons aussi l'innovation dans ce domaine et créerons les conditions d'une croissance durable.

En veillant à une transposition au plus proche des textes européens, nous limiterons les frictions juridiques et garantirons une concurrence loyale entre les entités couvertes par NIS 2 dans les différents États membres de l'Union européenne. Nous partageons, je le crois, cette ambition collective de relever notre niveau de cybersécurité et de renforcer la résilience de notre Nation. C'est un impératif majeur, presque existentiel.

Au regard des échanges que j'ai déjà pu avoir avec certains d'entre vous, je suis convaincue que nos débats à venir seront constructifs et que nous pourrons, grâce à ce texte, faire de la France un modèle en matière de résilience et d'innovation cyber.

M. Patrick Chaize, rapporteur. – Je vous remercie de votre présence parmi nous, madame la ministre. Nous attendions avec impatience la venue d'un membre du Gouvernement pour évoquer les enjeux de cybersécurité, mais nous n'osions plus l'espérer…

Le sujet est certes moins médiatisé que celui de l'intelligence artificielle, mais il n'en est pas moins urgent et primordial. En ma qualité de rapporteur chargé de l'examen du titre 2 de ce projet de loi, mon intervention sera centrée sur la transposition de la directive NIS 2. Au-delà de la hausse du nombre de secteurs et d'entités régulés, c'est un changement majeur de paradigme qui est à l'œuvre. Il ne s'agit plus seulement de sécuriser des infrastructures critiques, mais aussi d'assurer la résilience de l'ensemble du système d'information des entités critiques.

Depuis le début de l'année, je mène des auditions auprès de différents représentants sectoriels, experts de la cybersécurité et administrations. Je ne peux que témoigner de l'ampleur du chemin qu'il reste à parcourir pour une plus grande prise de conscience collective. Surtout, je ne peux que regretter le manque de communication autour de la transposition de la directive NIS 2. L'Anssi a pris de nombreuses initiatives, mais qu'en est-il du portage politique ? Que comptez-vous faire, madame la ministre, pour enfin donner à ce sujet la visibilité qu'il mérite ? Une campagne de communication institutionnelle ne serait-elle pas pertinente, pour les secteurs concernés, mais aussi pour toutes les entreprises et collectivités de France ?

Je me permets d'insister, car plus de 15 000 entreprises sont concernées, ainsi que l'ensemble des régions et des départements, près de 1 000 communautés de communes et 300 communes de plus de 30 000 habitants. Ces organisations devront elles-mêmes évaluer si elles sont soumises à la directive NIS 2, si elles sont des entités essentielles ou

importantes ; elles devront s'enregistrer auprès de l'Anssi et lui notifier leurs incidents de cybersécurité.

Toutes les auditions pointent dans la même direction : nous ne sommes pas prêts, alors que, paradoxalement, nous sommes déjà en retard aux yeux de la Commission européenne et en comparaison d'autres États membres. Il ressort également de nos travaux plusieurs points d'alerte, souvent récurrents et concordants, sur lesquels je souhaiterais avoir votre avis.

De façon assez inhabituelle pour notre pays, de nombreux acteurs dénoncent une sous-transposition de la directive et un projet de loi qui laisse une place trop importante aux dispositions de nature réglementaire. Par exemple, en cas d'incident, alors que la directive NIS 2 prévoit la transmission d'une alerte précoce dans un délai de 24 heures et la notification de l'incident dans un délai de 72 heures, le projet de loi contraint les entités à notifier leurs incidents sans délai et évoque la notification d'incidents critiques plutôt que d'incidents importants. Comment expliquez-vous ces différences qui peuvent nous paraître anodines, mais qui sont loin de l'être pour les entités concernées ?

À l'inverse, certains choix effectués sont assimilables à de la surtransposition, dont nous sommes beaucoup plus familiers dans notre pays. Par exemple, l'élargissement du périmètre des entreprises concernées par le projet de loi est régulièrement dénoncé, puisque des critères de taille et de chiffre d'affaires sont fixés alternativement, tandis que les textes européens les fixent cumulativement. Comment expliquez-vous ce choix ?

Enfin, le régime de contrôles et de sanctions exercés par l'Anssi est souvent perçu comme trop punitif et insuffisamment préventif. Les entités s'inquiètent du coût financier des contrôles réalisés par l'Anssi, qui seraient à leur charge, de l'absence de prise en compte du caractère intentionnel de la non-transmission d'informations à l'Anssi et de la rupture d'égalité induite par l'absence de sanctions prévues pour les administrations de l'État. Comment expliquez-vous ces choix qui paraissent discutables ?

M. Olivier Cadic, président. – Nous avons fait le calcul, plus de 40 décrets d'application sont prévus, ce qui est délicat pour le Parlement. Nous pouvons voir dans ce transfert au pouvoir réglementaire une sous-transposition, mais qui pourrait aussi devenir une surtransposition une fois les décrets parus.

Mme Clara Chappaz, ministre déléguée. – Nous faisons de la communication et de la sensibilisation un objectif majeur. L'Anssi a déjà accompli un travail important depuis 2023, mais nous comptons aussi sur l'impulsion du secteur déjà régulé, qui contribue depuis plusieurs années à élever le niveau de sécurité de nos infrastructures, et qui pourra aider l'Anssi à accompagner les nouvelles entités concernées.

Le Gouvernement doit également prendre toute sa part, j'en ai pleinement conscience, et nous travaillons à le faire de plusieurs manières.

J'étais présente à l'*European Cyber Week* qui s'est tenue récemment à Rennes. Nous travaillons aussi avec le campus cyber à l'organisation d'un événement afin de sensibiliser l'écosystème au sens large et avec l'Anssi à des campagnes de communication plus directes à destination des entités qui devraient, selon les différents modèles d'analyse, être concernées par le texte. Je rappelle que nous n'avons pas accès à toutes les informations permettant d'identifier les entreprises qui seront régulées.

Je fais aussi confiance aux fédérations professionnelles que j'ai pu rencontrer pour porter sur le terrain des messages de sensibilisation et d'accompagnement, et je vous suis bien entendu reconnaissante de relayer les attentes et interrogations que vous avez pu recueillir sur le terrain.

En matière de notification d'incident, l'article 17 du projet de loi impose aux entités mentionnées à l'article 14 de notifier sans retard injustifié à l'Anssi tout incident ayant un impact important sur la fourniture de leurs services. Dans certains cas prévus par la loi, notamment lorsque la divulgation de l'incident est dans l'intérêt public, l'Anssi peut, après avoir consulté l'entité essentielle ou importante concernée, exiger de celle-ci qu'elle informe le public de l'incident ou le faire elle-même.

Les critères d'appréciation de l'importance des incidents et les délais de notification seront précisés dans le décret en Conseil d'État d'application de la loi. L'Anssi travaille d'ores et déjà sur la notion d'incident « important » et sa définition réglementaire s'appuiera sur des critères objectivables, dans le prolongement de la réglementation en vigueur issue de la directive NIS 1. La directive NIS 2 précise elle-même certains de ces critères, mais la voie réglementaire nous semble la mieux à même de suivre l'évolution très rapide des menaces de cybersécurité. Quoi qu'il en soit, les textes réglementaires seront bien entendu soumis à consultation, comme ce fut le cas pour la définition des incidents dans le dispositif de sécurité des activités d'importance vitale prévu par la loi de programmation militaire.

S'agissant du risque de surtransposition de la directive NIS 2 que vous pointez en raison d'une différence de définition des entreprises de taille moyenne concernées, le décalage s'explique par le fait que l'article 2 du texte européen définit le champ des entreprises exclues de la directive, alors que le projet de loi délimite le champ des entreprises qui en relèvent. C'est pourquoi le critère cumulatif devient alternatif. La Belgique a suivi la même logique dans sa loi de transposition, et je peux donc vous rassurer sur ce point : le projet de loi ne vise que les seules entreprises qui dépassent les seuils fixés dans la directive. Le même raisonnement s'applique pour les entités importantes.

Sur la question des sanctions, le texte s'inscrit avant tout dans une logique d'accompagnement des entités vers une mise en conformité, la définition des sanctions permettant de matérialiser les conséquences attachées, à terme, à une non-conformité. À nos yeux, le projet de loi se

contente en la matière de transposer à l'identique les mesures de la directive NIS 2, qu'il s'agisse des contrôles, du régime de sanctions ou des amendes administratives. Je rappelle aussi que les taux d'amendes visés, 2 % du chiffre d'affaires pour les entités essentielles et 1,4 % pour les entités importantes, sont des seuils maximaux. La commission des sanctions ne prononcerait pas forcément de façon automatique les pourcentages qui ont été mentionnés.

Les entités essentielles peuvent également être soumises à une interdiction d'exercice, conformément au cadre de NIS 2, en cas de non-conformité. Enfin, il n'y aura pas de double sanction. La directive NIS 2 et le règlement général sur la protection des données (RGPD) étant très imbriqués, l'Anssi et la CNIL devront coopérer et s'informer en cas d'incident susceptible d'avoir un impact sur les données personnelles.

L'exclusion des sanctions pour les administrations nous semble proportionnée, celles-ci n'ayant pas les revenus et les moyens financiers des entreprises. Cela n'empêchera pas l'Anssi de mener un certain nombre de contrôles, et bien entendu des actions d'accompagnement et de sensibilisation.

M. Olivier Cadic, président. – Lorsqu'un hôpital privé peut être sanctionné, mais pas un hôpital public, il est difficile de ne pas y voir une forme d'inégalité.

M. Olivier Cadic, président, en remplacement de M. Hugues Saury**, rapporteur**. – L'économie du titre I^{er} du projet de loi qui vise à transposer la directive REC nous semble aller dans le bon sens. Lors des auditions que j'ai conduites, j'ai pu constater un consensus autour de la nécessité de renforcer le cadre normatif pour protéger les activités vitales de la Nation. Cependant, des préoccupations ont été exprimées, tant par les entreprises que par les collectivités territoriales, concernant l'accompagnement de l'État dans la mise en œuvre des obligations prévues par le projet de loi.

Pouvez-vous nous préciser les mesures envisagées pour soutenir les opérateurs d'importance vitale ainsi que ceux qui pourraient être amenés à intégrer ce dispositif avec l'entrée en vigueur de la loi ? En outre, dans un contexte budgétaire contraint, les services des ministères coordinateurs disposeront-ils de moyens suffisants pour assurer leurs missions actuelles et prendre en charge les nouvelles responsabilités qui leur incomberont ? L'étude d'impact du projet de loi reste en effet vague sur ce point, se contentant de mentionner que certaines dispositions entraîneront « une charge de travail supplémentaire pouvant avoir des impacts sur les ressources humaines ».

M. Olivier Cadic, président, en remplacement de M. Michel Canévet**, rapporteur**. – Sur la préparation du secteur financier à la mise en conformité avec Dora, beaucoup de retard a été pris pour la publication des normes de niveau 2. Or, les acteurs en ont besoin pour modifier leurs infrastructures informatiques ou encore pour renégocier les contrats avec leurs fournisseurs. Par ailleurs, beaucoup d'institutions financières déplorent le degré de détail

très élevé des normes RIS (*Retail Investment Strategy*), ce qui renchérit d'autant leur coût d'application.

Pouvez-vous vous mobiliser pour exiger des autorités européennes de supervision une meilleure visibilité sur le calendrier de publication de ces normes européennes, essentielles pour la bonne application de Dora ? À défaut, ne faudrait-il pas reporter l'entrée en vigueur de certaines dispositions ?

Le secteur financier étant soumis aux obligations de Dora, il serait souhaitable que, dans le projet de loi Résilience, les acteurs financiers soient bien explicitement exclus du statut d'entité essentielle prévu par la directive NIS 2.

À défaut, on assisterait à un empilement des couches d'exigences techniques et de déclarations qui comporterait un risque d'insécurité juridique pour les entreprises concernées. Pourquoi ne pas avoir explicitement prévu cette exclusion dans le projet de loi ?

Enfin, les sociétés de financement sont soumises aux obligations de Dora, alors même que cette catégorie d'acteurs n'est pas mentionnée dans la directive. Certes, un délai supplémentaire est accordé à ces sociétés jusqu'au 17 janvier 2026, mais ne faudrait-il pas adopter une approche plus proportionnée pour ces petites sociétés ? Une date d'entrée en vigueur au 1er janvier 2027 ne serait-elle pas plus réaliste ? Elle présenterait en effet l'avantage d'être très proche de celle fixée pour les autres entités financières similaires aux sociétés de financement dans l'Union européenne. L'Allemagne prévoit que les entités exerçant des activités de *leasing* seront soumises au cadre simplifié prévu par l'article 16 de Dora à partir du 1er janvier 2027.

Mme Clara Chappaz, ministre déléguée. – Vous m'interrogez sur les dispositifs d'accompagnement dont pourront bénéficier les opérateurs d'importance vitale, en particulier les collectivités territoriales. La sécurité des activités d'importance vitale repose sur une logique partenariale, même si elle n'exclut pas les contrôles. La directive REC prévoit de poursuivre les dispositifs actuels de soutien au moyen de plans types, de guides, d'exercices et de plans de protection externe pour leur permettre de se préparer en amont et de préparer aussi le concours des services de l'État en cas d'incident.

Un soutien à la formation des agents privés de sécurité est également prévu, de même que la fourniture d'outils de communication pour faciliter l'échange d'informations classifiées et la réalisation d'enquêtes administratives de sécurité au profit de l'opérateur.

Il me semble que cette logique d'accompagnement, qui est mise en œuvre depuis un certain temps maintenant par les structures compétentes de l'État, a fait ses preuves et que les retours sont positifs. Néanmoins, nous mettrons naturellement à jour les documents de planification.

Sur la question des budgets, nous n'avons pas été sensibilisés sur la nécessité de les revoir : en effet, les processus que je viens de décrire resteront les mêmes avec REC. Toute l'architecture d'accompagnement est déjà là. Certes, nous devrons mettre en place quelques éléments nouveaux, mais les budgets semblent suffisants pour absorber cette évolution. Pour autant, nous sommes évidemment prêts, comme je vous l'ai déjà indiqué, à procéder à de nouvelles consultations, si le besoin s'en fait sentir.

Dora s'applique depuis le 17 janvier dernier ; les acteurs financiers – banques, assurances, services de paiement… – le savent depuis longtemps et ils se devaient d'être prêts. Nous avons bien conscience qu'il existe encore des défis, mais cette échéance, fixée par le droit européen, est incontournable. Une autre échéance importante pour les entreprises concernées consiste à fournir aux autorités compétentes – ACPR et AMF –, au plus tard le 30 avril, les registres de leurs contrats de prestations. Ce *reporting* permettra aux instances européennes de désigner les partenaires et les prestataires informatiques critiques.

Les préoccupations dont vous vous êtes fait l'écho et que nous entendons également sur les délais, le manque de clarté ou le retard d'un certain nombre de normes sont davantage le reflet, à mon sens, d'un besoin de clarification, d'explication et de pédagogie plutôt que d'un strict problème de transposition. L'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF) ont publié des dossiers thématiques et des foires aux questions sur leurs sites internet. Il me semble que les différentes ressources mises à disposition répondent à une grande partie des questions que se posent encore certains acteurs.

La totalité des normes de NIS 2 a été finalisée, même si certaines publications officielles accusent un retard. La norme technique de réglementation (RTS selon l'acronyme anglais) sur le *reporting* des incidents informatiques et cyber devrait être publiée au journal officiel dans les prochains jours pour une entrée en vigueur vingt jours plus tard. La RTS sur l'harmonisation de la supervision est attendue sous peu, puisque le Parlement européen devait rendre son avis avant le 24 janvier.

En revanche, la Commission européenne a rejeté le standard technique de la sous-traitance, le texte doit donc être remanié par les autorités européennes de supervision et nous n'avons pas de date pour son entrée en vigueur.

Au total, ces différents retards n'ont pas d'incidence sur la transposition.

En ce qui concerne le coût de la mise en conformité, les entités concernées ont déjà un niveau de maturité avancé en matière de cybersécurité et de risques. Loin de moi l'idée de minimiser ce coût, notamment en termes de mises à jour technologiques, de recrutement ou de tests de pénétration, mais il faut le rapporter à celui des attaques physiques ou cyber…

En ce qui concerne l'articulation entre NIS 2 et Dora, cela résulte d'un héritage européen et nous avons eu des échanges nourris avec l'AMF, l'ACPR, l'Anssi et l'ensemble des parties prenantes pour nous assurer que les frictions éventuelles seront minimisées pour les entités soumises aux deux textes. Même les entités couvertes par Dora doivent s'assurer que leurs systèmes d'information qui sont utilisés par des millions de Français respectent les référentiels de NIS 2. Les deux textes sont en fait complémentaires et sortir certaines entités de NIS 2, au motif qu'elles respectent Dora, ferait prendre un risque aux Français lorsqu'ils utilisent des services financiers.

Le sujet des sociétés de financement est particulier à la France. Le délai d'un an, jusqu'à 2026, nous semble réaliste pour ces sociétés, qui ont été consultées à ce sujet et qui, me semble-t-il, n'ont pas soulevé de problème spécifique. La principale différence entre une société de financement et un établissement de crédit réside dans le fait que la société de financement ne peut effectuer, dans les conditions et limites de son agrément, que des opérations de crédit, alors que l'établissement de crédit à la fois délivre des crédits et reçoit des fonds remboursables. Il n'y a donc pas dans le texte de surtransposition, mais le reflet d'une pratique courante ; ce n'est d'ailleurs pas la première fois que cette question est soulevée dans le cadre d'une telle transposition.

Pour nous, les exigences de Dora doivent être étendues aux sociétés de financement pour deux raisons : d'une part, harmoniser les exigences en matière de gestion du risque cyber entre les différentes structures qui assurent le même service ; d'autre part, préserver la stabilité financière en garantissant une protection cyber.

Le secteur financier est une cible privilégiée pour des attaques cyber et ces attaques effritent particulièrement la confiance de nos citoyens dans la sécurité de nos infrastructures critiques. C'est pourquoi nous avons jugé utile d'ajouter les sociétés de financement au texte.

M. Michel Canévet, rapporteur. – Je remercie le président de la commission spéciale d'avoir relayé mes premières questions.

Pour les entreprises qui sont concernées à la fois par Dora et par NIS 2, il sera très difficile de retenir une méthodologie pertinente pour mettre en œuvre des obligations qui sont différentes. Il faut prendre ce problème concret en compte.

Par ailleurs, vous savez certainement, madame la ministre, que le Sénat entend le plus possible éviter les surtranspositions. Or c'est clairement le cas pour les sociétés de financement. Il ne peut évidemment être question de méconnaître les risques cyber, mais intégrer ces sociétés pose des difficultés particulières : d'une part, hormis deux gros acteurs, il s'agit de structures de petite taille pour lesquelles le coût du processus sera élevé ; d'autre part, ce marché est particulièrement concurrentiel au niveau européen et international et nous ne pouvons pas mettre des boulets aux pieds de nos seules entreprises.

Je voudrais enfin évoquer la question du *reporting*. Aujourd'hui, l'Anssi est organisée pour assurer un *reporting* permanent. Est-ce que les autres acteurs qui seront demain concernés – l'AMF, l'ACPR – en seront capables ? Comment se préparent-ils à cette mission ?

Mme Clara Chappaz, ministre déléguée. – Pour les sociétés de financement de petite taille, la question du délai d'un an pour la mise en conformité – nous en avons déjà parlé – a été abordée lors des consultations : ce délai permet de répondre au besoin que vous exprimez. Nous avons réalisé une étude à ce sujet : 135 sociétés sont concernées par cette mise en conformité, dont une dizaine de taille telle qu'elles devront être en conformité dès l'entrée en vigueur de la loi, les autres bénéficiant donc d'un délai d'un an. Nous procéderons à de nouvelles consultations, si cela est nécessaire.

S'agissant de l'articulation entre NIS 2 et Dora, l'Anssi travaille avec l'AMF et l'ACPR pour établir des *guidelines* pertinentes. Le périmètre des entités régies par Dora est plus petit que celui de NIS 2 et nous travaillons pour éviter les lourdeurs de mise en œuvre et de gestion, ainsi que les doubles contrôles. Nous ne voulons pas alourdir les processus de *reporting*, de contrôle ou de mise en conformité.

Enfin, sur votre dernière question, vous avez raison de mettre l'accent sur la nécessité de nous organiser pour internaliser certaines contraintes, en particulier en termes de cellules de veille. Cela va naturellement prendre du temps, mais nous sommes sur la bonne voie.

M. David Ros. – Madame la ministre, vous êtes venue vendredi dernier dans l'Essonne, sur le plateau de Saclay, pour le lancement de neuf *clusters* autour de l'intelligence artificielle. Or ce département a été victime de plusieurs cyberattaques importantes : au centre hospitalier Sud Francilien, à l'hôpital d'Orsay et récemment à l'université Paris-Saclay. Cette dernière attaque a paralysé le début de l'année universitaire ; je me félicite donc que les établissements d'enseignement menant des activités de recherche soient mentionnés, dans l'article 8 du projet de loi, parmi les entités essentielles.

La prévention, la pédagogie et l'information sont des aspects très importants de la lutte contre la cybercriminalité. Or, d'une part, le nombre des attaques augmente ; d'autre part, il faut souvent remettre en service de manière urgente les systèmes attaqués, en particulier lorsque cela paralyse l'activité de l'établissement concerné. Les moyens seront-ils suffisants pour tout cela ?

Se défendre, c'est bien, mais contre-attaquer, c'est mieux ! Pour cela, les activités de recherche sont très importantes et l'intelligence artificielle peut sûrement nous aider. Est-ce que des études sont menées dans ce sens ?

Mme Hélène Conway-Mouret. – Selon certaines estimations, la France serait le quatrième pays le plus touché par des cyberattaques, le deuxième selon le Medef. J'ajoute que 60 % des entreprises qui subissent une attaque déposent le bilan dans les six mois qui suivent.

Je voudrais vous interroger particulièrement sur les petites entreprises qui ne sont pas concernées par ce texte, puisqu'il établit un seuil de mise en conformité relativement élevé – 50 employés selon l'article 9 du projet de loi pour être qualifiée d'entité « importante ». Or, par exemple dans le secteur de la défense, auquel notre commission des affaires étrangères, de la défense et des forces armées est particulièrement attentive, beaucoup de fournisseurs de grands groupes sont de petite taille, mais font pourtant preuve d'une grande innovation et œuvrent dans des domaines sensibles. Ces petites entreprises sont absolument essentielles à notre écosystème économique et militaire et à notre souveraineté et elles ont, elles aussi, besoin d'un niveau de protection très élevé, mais elles ne disposent pas d'une trésorerie suffisante pour se protéger correctement. Elles souffrent aussi d'un manque d'informations.

Au-delà de ce projet de loi, avez-vous défini, madame la ministre, une politique volontariste pour accompagner ce type d'entreprises qui sont victimes à la fois de rackets et de vols de technologie, ce qui est particulièrement grave ? Il faut aussi penser à protéger les personnels qui utilisent des ordinateurs portables.

Mme Michelle Gréaume. – Selon l'article 10 du projet de loi, le Premier ministre pourra désigner comme entité essentielle ou importante une entité exerçant une activité relevant d'un secteur d'activité hautement critique ou critique. Quelles entités envisagez-vous dans cet article ?

L'article 17 concerne l'obligation de notification par les personnes concernées de tout incident ayant un impact important sur la fourniture de leurs services. Au-delà de la notification, ce qui est important, c'est le suivi des notifications et les réactions des autorités, y compris le week-end ou en cas d'attaques massives simultanées.

L'article 41 modifie le code des postes et des communications électroniques pour renforcer les sanctions. Comment comptez-vous préserver les systèmes d'information de La Poste, un service public auquel les Français sont très attachés ? Quelles seront les conséquences sur l'efficacité du service ?

Certains métiers vont disparaître avec l'intelligence artificielle ; d'autres vont se créer. Des études ont-elles été réalisées quant aux conséquences à court et moyen terme sur l'emploi du développement de l'intelligence artificielle ?

M. Akli Mellouli. – Les directives européennes dont nous parlons vont élargir le public concerné par des obligations en termes de cybersécurité. Existe-t-il un programme national pour sensibiliser et former les Français ?

Dans ce type de politique, l'évaluation est très importante. Comment sera mesuré l'impact de cette loi et quels mécanismes permettront d'ajuster les obligations, si cela s'avère nécessaire, dans les prochaines années ?

Comment renforcer la coopération entre l'État et le secteur privé dans la mise en œuvre des exigences de cybersécurité ?

M. Olivier Cadic, président, en remplacement de Mme Vanina Paoli-Gagin. – Notre collègue Vanina Paoli-Gagin a dû partir, mais elle m'a demandé, madame la ministre, de vous poser deux questions.

Est-ce l'innovation en *open source*, la diversification des fournisseurs de *cloud* ou bien les deux qui nous permettront une meilleure gestion proactive des risques cyber protéiformes que vous nous avez exposés ?

Comment va-t-on pouvoir mobiliser les financements nécessaires pour assurer l'*upgrading* – en bon français… – de l'ensemble des infrastructures ?

Mme Clara Chappaz, ministre déléguée. – L'Anssi a naturellement un rôle de chef de file en matière de prévention et de pédagogie, mais on ne doit pas oublier le formidable travail réalisé en la matière par l'ensemble des acteurs de notre écosystème. Le Gouvernement doit bien sûr prendre toute sa part dans la sensibilisation et la communication autour des sujets cyber ; il est évident que le sujet de l'IA nous mobilise particulièrement, notamment à l'approche du sommet international que la France va bientôt accueillir, mais cela n'enlève rien à l'importance de la question de la cybersécurité sur laquelle nous restons également engagés.

D'ailleurs, l'IA peut apporter beaucoup à la cybersécurité : récemment, je me suis rendue à Rennes, dans le cadre de l'*European Cyber Week*, pour évoquer le projet SequoIA qui est développé dans un cluster de l'université de la ville. Nous avons lancé à cette occasion un nouvel appel à projets sur les technologies critiques innovantes.

S'agissant des moyens de l'Anssi, vous savez, puisque vous avez auditionné son directeur, que l'agence bénéficie d'une trajectoire d'augmentation continue de ses équivalents temps plein (ETP) depuis 2022, ce qui reflète le soutien que le Gouvernement entend lui apporter. Elle exerce déjà plusieurs des missions qui sont énumérées dans NIS 2 et ses responsables ont estimé les besoins en agents liés à la mise en œuvre des directives à 50 ETP. Or le délai de mise en conformité est de trois ans, tandis que la trajectoire dont je parlais prévoit une progression des ETP de 40 par an. L'agence devrait donc pouvoir absorber la montée en puissance de ses nouvelles missions au fur et à mesure et conformément au calendrier fixé.

S'agissant des petites entreprises sous-traitantes, je vous rappelle que le référentiel de l'Anssi fixe des *guidelines* pour leur mise en conformité et qu'il existe un effet d'entraînement avec les entreprises donneuses d'ordre. Dans le secteur de la défense plus particulièrement, le ministère des armées a mis en place des parcours cyber dédiés.

J'ajoute, comme cela a été dit, que le Premier ministre peut désigner une entité afin qu'elle soit assujettie aux obligations de NIS 2, même quand

elle ne remplit pas les critères en termes de nombre d'employés ou de chiffre d'affaires, par exemple des hôpitaux ou des laboratoires de recherche.

Madame Gréaume, je ne pense pas que nous ayons le temps de débattre aujourd'hui des liens entre l'IA et l'emploi : c'est un sujet passionnant et je pourrais en parler des heures…

En ce qui concerne les budgets informatiques, il est absolument nécessaire que les entreprises et tous les organismes de manière générale intègrent les questions de cybersécurité dans leurs dépenses courantes, parce que la menace est forte et qu'elle évolue en permanence. Ce sont des dépenses récurrentes, pas temporaires !

Vous avez aussi évoqué l'article 41 qui a trait notamment au dispositif de sanctions à la main de l'Agence nationale des fréquences (ANFR) en matière de lutte contre le brouillage des fréquences. Cette question tient également une place essentielle dans la continuité des activités économiques et étatiques. Le nombre des cas de brouillage et leur gravité augmentent depuis quelques années, ce qui altère le bon fonctionnement des applications qui utilisent des ressources hertziennes. Un rapport d'inspection a présenté une série de recommandations pour sécuriser ces fréquences et il nous a semblé adéquat d'inscrire dans la loi des sanctions graduées avec des quantums de peine plus élevés pour rendre la dissuasion plus efficace. Il existe aujourd'hui une forme de sentiment d'impunité en la matière et nous voulons y mettre fin avec ce texte.

M. Olivier Cadic, président. – Pourquoi les missions de l'Autorité nationale inscrites dans la première version du texte sont-elles maintenant renvoyées à un décret en Conseil d'État ?

À quelles autres entités l'article 5 fait-il référence, lorsqu'on parle d'activités « dans le domaine de la défense » ?

Patrick Chaize vous a interrogé sur la qualification des incidents, qui est précisée dans la directive, mais cela reste un mystère pour moi : pourquoi les autres pays inscrivent-ils la définition des incidents dans la loi, alors que le Gouvernement renvoie cela à un décret ?

La directive NIS 2 prévoit, dans son article 10, que les États membres veillent à ce que « chaque Centre de réponse aux incidents de sécurité informatique (CSIRT) dispose de ressources suffisantes pour pouvoir s'acquitter efficacement de ses tâches ». Comment le Gouvernement a-t-il prévu d'assurer la pérennité financière des centres régionaux ? Ces centres régionaux sont-ils concernés par l'article 11 de la directive ?

Certains interlocuteurs nous ont alertés sur l'insertion, dans l'article 14 du texte, de SecNumCloud : pour eux, cela pourrait entraver l'harmonisation européenne des normes de sécurité. Quelles sont les intentions du Gouvernement à cet égard ?

Lors de notre déplacement en Belgique, nous avons été marqués par la clarté de la position des autorités belges. Par exemple, si une entité est certifiée ISO 27001, elle est réputée conforme, parce que cette norme inclut les problématiques humaines – or on sait que 80 % des problèmes de cybersécurité sont liés à une erreur humaine. Que pensez-vous de cette position de la Belgique ?

Vous avez évoqué le GIP ACYMA (Groupement d'intérêt public Action contre la cybermalveillance). Finalement, comment voyez-vous l'articulation entre les différents acteurs ?

Enfin, le projet de loi renvoie fréquemment au pouvoir réglementaire, mais qui va contrôler l'administration ?

Mme Clara Chappaz, ministre déléguée. – Nous avons discuté avec l'Anssi des normes belges, mais nous avons une différence d'approche avec ce pays. Nous privilégions des objectifs de sécurité et de protection face à la menace cyber, quand la Belgique envisage la conformité par le prisme du management.

S'agissant des entités essentielles, nous avons voulu rester proches de NIS 1 et des dispositions du code de la défense pour éviter des changements trop brutaux qui auraient eu un coût élevé. Pour autant, nous étudions – le directeur de l'Anssi en parlerait mieux que moi – la mise en place de mécanismes de reconnaissance mutuelle pour faciliter l'activité des entreprises concernées.

Sur l'article 14, nous n'avons pas prévu d'y intégrer SecNumCloud, parce que, dans la directive européenne, il n'est pas fait mention de certification au niveau du *cloud* et que nous ne voulons pas surtransposer. Nous devons travailler sur un cadre européen de sécurité du *cloud*, mais ce n'est pas l'objet de ce texte.

Les CSIRT territoriaux seront bien des organismes de proximité, mais l'idée de l'Anssi est qu'il faut partir de la victime : peu importe vers qui elle se tourne, elle doit recevoir le même niveau de réponse. Il revient à l'Anssi d'organiser le travail entre les différents acteurs sans que cela pèse en aucune façon sur les victimes.

En ce qui concerne la définition des incidents, cela relève aussi, au niveau de l'Union européenne, de ce que nous appelons en France le pouvoir réglementaire, puisqu'il s'agit d'un acte délégué. Il faut pouvoir faire évoluer la définition au gré de l'évolution des menaces. Voilà pourquoi nous devons garder de la flexibilité, mais tout cela sera naturellement décidé après consultations. Il en était de même dans NIS 1.

Je ferai la même réponse pour la définition des missions des autorités – c'était votre première question, monsieur le président. Nous faisions ainsi dans le cadre de NIS 1 et le Conseil d'État a été d'avis qu'il fallait faire de même ici.

M. Olivier Cadic, président. – Madame la ministre, je vous remercie.

MARDI 4 FÉVRIER 2025

Table ronde avec les associations d'élus (Association des maires de France, association des départements de France, association des régions de France, intercommunalités de France et Métropole du Grand Paris)

M. Olivier Cadic, président. – Notre cycle d'auditions publiques consacrées au projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité se poursuit aujourd'hui par une table ronde avec les associations d'élus sur le thème de la cybersécurité et des collectivités territoriales.

Plusieurs raisons ont conduit à organiser cet échange avec les différents échelons de collectivités.

La première tient à ce que le projet de loi dont notre commission spéciale est saisie vise à élever le niveau de cybersécurité des collectivités de plus de 30 000 habitants dans le cadre de la transposition de la directive européenne relative aux mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite NIS 2 (*Network and Information Security 2*).

Un deuxième motif est celui de la vulnérabilité numérique de nos services publics territoriaux, qui se trouvent en première ligne au même titre que les hôpitaux, dont les attaques sont cependant plus médiatisées. Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), les attaques réussies par rançongiciels sur des collectivités représentent même un quart de l'ensemble des attaques, contre 10 % sur les établissements de santé. C'est pourquoi le retour d'expérience de nos associations d'élus nous sera précieux pour apprécier le juste seuil et le juste niveau d'obligation à inscrire dans la loi.

Enfin, troisième raison de cette table ronde, certaines collectivités territoriales sont elles-mêmes des actrices de la cybersécurité en proposant soit des actions de prévention, soit des dispositifs spécifiques ; je pense aux régions qui se sont engagées dans la création de centres de réponse aux incidents de sécurité informatique (Csirt, *Computer Security Incident Response Team)* afin de soutenir les entreprises de leurs territoires face à de tels incidents. Leur rôle est diversement connu et reconnu. Aussi, le témoignage de représentants des régions nous sera utile pour discerner les différentes approches proposées à leur sujet par l'Anssi, la ministre déléguée chargée de l'intelligence artificielle et du numérique, et les entreprises expertes en cybersécurité, qui ne partagent pas la même appréciation de leurs missions.

M. Michel Sauvade, vice-président du conseil départemental du Puy-de-Dôme, maire de Marsac-en-Livradois, représente l'Association des maires de France et des présidents d'intercommunalité (AMF) ainsi que Départements de France.

M. Jérôme Tré-Hardy, conseiller régional de Bretagne – qui nous avait reçus, mon collègue rapporteur pour avis sur les crédits du programme 129 relatifs à la cybersécurité du projet de loi de finances (PLF) pour 2025 et moi-même, à Rennes au pôle d'excellence cyber – et Mme Constance Nebbula, vice-présidente de la région des Pays de la Loire chargée du numérique, représentent l'association Régions de France. Vous êtes les acteurs les mieux placés pour nous relater vos expériences respectives de la création des Csirt régionaux. Vous êtes accompagnés de Mme Laure Prévot, conseillère économie à Régions de France.

Pour Intercommunalités de France, nous recevons Mme Marlène Le Dieu de Ville, vice-présidente chargée du numérique, par ailleurs vice-présidente déléguée à l'économie numérique, aux systèmes d'information et à la culture de la communauté de communes de Lacq-Orthez. Vous accompagne Mme Montaine Blonsard, responsable des relations avec le Parlement d'Intercommunalités de France.

Enfin, pour la métropole du Grand Paris, nous recevons à sa demande M. Geoffroy Boulard, maire du XVII^{e} arrondissement, conseiller de Paris et vice-président de la métropole du Grand Paris, accompagné de Mme Justine Terzi, chargée de mission cyber, et de M. Eloy Lafaye, chef de projet innovation numérique de la métropole.

Nous vous remercions très sincèrement d'avoir répondu à notre invitation pour partager votre point de vue sur le projet de loi et les conséquences de cette transposition pour les entreprises. Nous serons en particulier intéressés par les dispositions du texte qui vous posent un problème et vos éventuelles propositions de modification.

Avant de vous céder la parole, je rappelle que cette audition fait l'objet d'une captation vidéo disponible en ligne sur le site du Sénat.

Je vous propose pour ouvrir notre table ronde que chaque organisation nous présente sa position sur le texte de projet de loi. Je donnerai ensuite la parole à nos rapporteurs, puis à ceux de nos collègues qui le souhaiteront.

M. Michel Sauvade, vice-président du conseil départemental du Puy-de-Dôme, maire de Marsac-en-Livradois, représentant de l'Association des maires de France et des présidents d'intercommunalité (AMF) et de Départements de France. – Je vous présenterai successivement les positions respectives de l'AMF et de Départements de France. Elles présentent entre elles, comme avec celles des autres associations d'élus, de nombreux points communs, mais également des différences.

Pour ce qui a trait à l'AMF, si ses membres partagent l'ambition d'un renforcement de la cybersécurité des communes et des établissements publics de coopération intercommunale (EPCI), ils expriment leur vive inquiétude sur les conditions dans lesquelles ils devront mettre en œuvre les nouvelles obligations, qui seront coûteuses, tant sur le plan financier, dès cette année, que sous l'angle humain et matériel, avec de fortes tensions attendues sur la filière des métiers de la cybersécurité. L'AMF s'interroge par ailleurs sur le périmètre réel des communes concernées, qui ne semble pas clair dans le projet de loi actuel, notamment du fait des rapports étroits que ces dernières entretiennent avec leurs EPCI. L'AMF estime que la transposition de la directive NIS 2 ne doit pas ignorer cette réalité, en s'inscrivant dans une double logique de transition progressive et d'accompagnement fort de l'État.

L'association tient en tout premier lieu à souligner la qualité de la concertation menée avec l'Anssi dès la fin de l'année 2023, l'article 5 du titre II du projet de loi rappelant que le Gouvernement charge l'agence de la mise en œuvre de sa politique en matière de sécurité des systèmes d'information. Cependant, l'audition devant votre commission de la ministre déléguée ne nous a pas rassurés sur le niveau d'implication politique du Gouvernement à notre égard. Si la ministre a évoqué à plusieurs reprises les fédérations professionnelles, les collectivités territoriales ont en revanche semblé quelque peu absentes de son champ de vision.

L'AMF est soucieuse de la question de la cybersécurité et souhaite que l'application de la directive européenne soit un succès, en réussissant à inscrire les communes et les EPCI dans une dynamique commune avec les autres niveaux de collectivités locales. Pour ce faire, il importe que le législateur tienne compte des moyens des communes et des EPCI, de sorte que la mise en œuvre des nouvelles mesures soit supportable financièrement et faisable techniquement.

À cet égard, l'AMF regrette l'absence d'étude d'impact sur les conséquences de la transposition, surtout dans le contexte actuel d'incertitude financière. Un rapport du cabinet de conseil Idate rendu public au mois de novembre 2024 estime que le coût pour les collectivités locales des solutions de sécurité nécessaires à leur mise en conformité avec la directive NIS 2 s'élèverait à 690 millions d'euros par an. S'y ajouteraient 105 millions d'euros par an au titre de l'embauche et de la formation de ressources humaines qualifiées. Les nouvelles obligations emportent de nombreuses conséquences sur un plan tant organisationnel que financier.

Autre source d'inquiétude, leur non-respect pourra engager la responsabilité du maire ou du président d'EPCI. Entre sanctions contre les collectivités et sanctions contre les services de l'État, que penser ici de la réponse ambiguë apportée par la ministre Clara Chappaz lors de son audition devant vous, qui semblait en même temps adhérer et s'opposer à l'avis du Conseil d'État ?

Sans étude d'impact, l'AMF n'a pas été en mesure de se prononcer sur les périmètres proposés. Certains parmi nous se sont même interrogés – légitimement de mon point de vue – sur le rapport coût-risque pour les collectivités. L'association n'en a pas moins fait connaître à plusieurs reprises à l'Anssi et aux représentants de l'État ce qu'elle juge être des points de vigilance :

- premièrement, le risque de tension sur les métiers de la cybersécurité, qui influera sur le recrutement de professionnels au sein de nos collectivités, avec, en conséquence, l'éventuel recours onéreux à des prestataires extérieurs ;

- deuxièmement, Patrick Molinoz et moi-même, qui coprésidons la commission numérique de l'AMF, mettons en évidence avec des directeurs des systèmes d'information et des responsables sécurité des systèmes d'information (RSSI) la très grande fragilité de nos structures, en raison à la fois d'un portage politique qui reste faible à notre échelle et des enjeux en présence ;

- troisièmement, la nécessaire progressivité de l'entrée en application des nouvelles obligations, pour des raisons évidentes de coût et de difficultés de gestion des ressources humaines, alors que communes et EPCI sont appelés à maîtriser leurs dépenses ; l'accompagnement financier de l'État, mais aussi des régions et des départements, s'avère indispensable.

Une inquiétude particulière porte par ailleurs sur les plus petites communautés de communes et sur leur capacité à respecter les obligations du futur référentiel de cybersécurité.

Enfin, l'incertitude prévaut sur les conséquences réelles de ces nouvelles normes pour les systèmes d'information des communes membres des intercommunalités, puisque toutes partagent entre elles des services, serveurs et logiciels.

En ce qui concerne Départements de France, la qualité des consultations conduites avec l'Anssi est de nouveau mise en évidence, de même que l'absence d'écho véritable, à l'échelon politique, des préoccupations que les collectivités membres ont exprimées. Ces préoccupations portent sur trois aspects : les ressources nécessaires à la réussite du redimensionnement et de la mise à l'échelle des systèmes d'information, la structuration territoriale d'une politique publique de cybersécurité, le soutien de l'État.

Du point de vue de Départements de France, le texte du projet de loi consiste en une transposition brute de la directive européenne. D'une part, il ne répond pas à ses préoccupations ; d'autre part, il renvoie un grand nombre de dispositions au niveau réglementaire, sans en fixer suffisamment les principes. Il fait ainsi courir le risque de voir la mise en conformité administrative prévaloir par rapport au développement de mesures véritablement opérationnelles. Cette observation souligne combien la

connaissance des enjeux de la cybersécurité se situe d'abord à cette échelle des départements.

Dans le détail, les inquiétudes de Départements de France concernent en premier lieu les effets des nouvelles mesures sur les pratiques de sécurité informatique. De telles mesures supposent en effet une adaptation de toute la chaîne de promotion de la cybersécurité : gouvernance, gestion des risques et des incidents, obligations de rapport et de notification, sécurité de la chaîne logistique ou de soutien, sécurisation de la maintenance des systèmes, pratiques fondamentales en matière d'hygiène cyber, matériel et technologies embarquées, notamment la cryptographie et le chiffrement, formation, sécurité du personnel et des politiques de contrôle d'accès.

En matière financière, les évolutions demandées emporteront de lourdes conséquences, tant en dépenses d'investissement qu'en dépenses de fonctionnement, alors que les budgets des départements sont déjà fortement contraints. Les crédits relatifs à l'informatique semblent ainsi être, en 2025, amputés de l'ordre de 30 % à 50 % en moyenne dans la plupart de nos collectivités.

Sur le plan humain, il sera nécessaire de recruter et de former les agents disposant des compétences adéquates. L'offre de formation représente un enjeu à part entière. Elle implique la structuration d'une filière professionnelle de cybersécurité. Si un certain nombre d'initiatives sont déjà engagées en ce sens, les départements sont confrontés sur le marché de l'emploi à la concurrence d'importants acteurs privés. À titre d'exemple, le conseil départemental du Puy-de-Dôme a vu le départ de 23 agents au cours des trois dernières années, au sein de sa direction des systèmes d'information (DSI), qui comprend 45 postes. Il a procédé à douze recrutements et onze postes restent encore à pourvoir. L'enjeu est celui de notre fragilité en matière de cybersécurité et, au-delà, de notre fonctionnement au quotidien.

L'association Départements de France est par ailleurs attentive aux effets de la transposition sur la chaîne de responsabilités. La mise en conformité avec la directive NIS 2 passera nécessairement par le recours à des prestataires de services de confiance. Elle impliquera une révision des marchés et, surtout, une évaluation des différents prestataires par les commanditaires, laquelle nous pose évidemment un problème. Bien que le règlement européen sur la cyber-résilience (*Cyber Resilience Act*, CRA) impose la conformité de tous les produits numériques, la question des moyens de certification des prestataires reste en effet posée. Les présidents de département ne pourront pas se porter garants de tous les prestataires ; la législation ou la réglementation doivent prévoir le partage des responsabilités. Peut-être une déclaration de conformité offre-t-elle ici une piste de réflexion à approfondir.

Autre point non négligeable, les départements devront s'adapter rapidement aux nouvelles réglementations, ce qui peut s'avérer difficile dans un environnement technologique par ailleurs en constante évolution.

Encourager la coopération et le partage d'informations, ce que l'on retrouve aux articles 23 et 24 du projet de loi, est évidemment louable. Cependant, l'une et l'autre nous paraissent présentés de façon très centralisée et limitée. Pour sa part, Départements de France a organisé dès février 2023, à huis clos, un séminaire des présidents afin d'échanger sur les cyberattaques et de créer collectivement un plan de cyber-résilience. Celui-ci a été publié en juin 2023. Un groupe des RSSI a été mis en place au moyen d'une plate-forme collaborative, en lien étroit avec le Club des RSSI des collectivités. En outre, le secrétariat général de la défense et de la sécurité nationale (SGDSN) et l'Anssi ont été sollicités plusieurs fois en vue d'intervenir devant les présidents comme devant les directeurs des services généraux des conseils départementaux pour optimiser la prise en compte de la cybersécurité dans la gouvernance de ces collectivités. Enfin, Départements de France met en place un groupe de contact constitué de directeurs des systèmes d'information, de RSSI et de directeurs des services généraux, en prévision d'échanges avec l'Anssi sur l'importante partie réglementaire à venir, lorsque le projet de loi sera adopté.

La réflexion conduite par Départements de France porte sur la structuration d'une politique publique territoriale de cybersécurité. Parmi les conditions d'une mise à l'échelle réussie des systèmes d'information figure la consolidation d'un réseau territorial de cybersécurité. Ce réseau repose aujourd'hui essentiellement sur les Csirt, créés par les régions. De son côté, l'État dispose du réseau des délégués territoriaux de l'Anssi, qui sont au nombre d'un ou deux par région. Les unités spécialisées des forces de sécurité intérieure restent quant à elles centralisées au niveau national. C'est clairement insuffisant et aucune perspective favorable ne se dessine. L'étude d'impact relative au projet de loi n'évoque ainsi, sur l'augmentation des moyens mis à disposition de l'Anssi, qu'une soixantaine d'équivalents temps plein (ETP) supplémentaires pour une montée en charge considérable du nombre d'entités à superviser.

Là où ils existent, les campus cyber font leurs preuves. Leur existence et leur dynamisme reposent sur l'énergie de chaque acteur. Il est dommage que le texte, par une transposition assez sèche des obligations de la directive européenne, ne leur donne pas d'autre impulsion.

Enfin, Départements de France attire l'attention sur le coût des contrôles conduits par l'Anssi qui, semble-t-il, doit revenir à la charge des entités contrôlées. Cela nous paraît totalement inacceptable, quand bien même ces contrôles n'interviendraient qu'en cas de suspicion forte de non-respect des règles. Il s'agirait alors d'une sanction par avance et je rappelle l'avis que le Conseil d'État a rendu sur la question. On peut par ailleurs s'interroger sur l'exonération que l'État prévoit pour ses propres services.

Mme Constance Nebbula, vice-présidente de la région des Pays de la Loire chargée du numérique, représentante de Régions de France. – Avant toute chose, je vous remercie d'interroger les associations de collectivités territoriales et de prendre le temps de recueillir le point de vue des élus locaux.

Par leur importance, par leur nombre d'administrés, par le niveau de criticité des données qu'elles récoltent et traitent, les régions seront considérées comme « entités essentielles » au sens du projet de loi et devront donc répondre aux critères de sécurité les plus élevés de la nouvelle directive NIS 2, directive sur laquelle je concentrerai mon intervention.

Le volume des cyberattaques menées contre les collectivités ne cesse de croître. Douze des dix-huit régions françaises ont été touchées, pour certaines très durement, et les collectivités comme d'autres structures publiques, telles que les établissements de santé, sont devenues des cibles. Dans ces conditions, et considérant que les régions occupent une place centrale dans le domaine de la cybersécurité, nous portons un vif intérêt à ce texte du projet de loi.

Comme l'AMF et Départements de France, nous avons été associés dès novembre 2023 aux travaux de l'Anssi préalables à la transposition de la directive européenne. Nous avons demandé à l'Agence une étude d'impact sur cette transposition, laquelle n'a jamais été réalisée. Nous avons également demandé une estimation des coûts qu'elle induirait pour les régions, afin de mesurer le rapport bénéfice-risque de ses dispositions, dans un contexte budgétaire particulièrement tendu où des arbitrages doivent intervenir et où il importe de mobiliser les élus sur les moyens financiers à accorder prioritairement.

Une difficulté existe quant à la prise en compte des obligations de la directive NIS 2, 23 % des 500 décideurs informatiques interrogés dans la dernière édition du baromètre sur la maturité cyber des collectivités reconnaissant n'en avoir jamais entendu parler et seuls 24 % d'entre eux se déclarant prêts à les appliquer. La marge de progression est donc importante, le manque de connaissances et de préparation patent.

En ce qui concerne l'Anssi, je distinguerai entre son niveau national et son niveau régional. Régionalement, nos contacts sont plutôt de qualité et le dialogue est régulier, quoique les moyens restent faibles. En revanche, nous constatons un discours quelque peu différent au niveau national.

La question du financement et de la pérennité des Csirt se pose. L'Anssi avait octroyé aux régions 1 million d'euros pour leur création pendant trois ans. Les régions se sont mobilisées en ce sens et presque toutes à présent en disposent. Néanmoins, depuis lors, aucune affirmation nouvelle de la politique publique de cybersécurité n'est intervenue à l'endroit des régions. Je me suis entretenue mardi dernier avec Mme Chappaz, au terme de son audition devant vous, et je lui ai appris que les régions ne disposaient pas de la compétence en matière de cybersécurité…

Régions de France souhaite obtenir une clarification sur cette compétence, laquelle suppose des financements. Au titre des financements, l'association demande que le renforcement de la cybersécurité des collectivités territoriales et des administrations publiques soit mieux intégré au plan France 2030, afin d'obtenir un accompagnement financier à la hauteur du niveau de mise en conformité attendu.

Aujourd'hui, les moyens font défaut. En 2021, le Gouvernement a certes mis en place une ambitieuse stratégie d'accélération cyber. Cependant, sur le montant de 1,7 milliard d'euros qu'elle recouvre, dont 720 millions d'euros d'argent public, 136 millions sont affectés au travail d'animation par l'Anssi, dont 60 millions d'euros pour créer des Csirt ; et les régions n'ont en définitive obtenu que 1 million d'euros pour trois ans, sans autre garantie de financement au terme de cette période. Elles n'apparaissent ainsi associées ni financièrement, ni humainement, ni politiquement à la suite qui sera donnée.

Quant aux campus cyber, si l'initiative est nationale, elle ne s'est concrètement traduite, contrairement à ce qui avait été annoncé, par aucune aide en faveur des régions. Chaque région a dû s'en occuper seule, à moyens et périmètre constants, raison pour laquelle, d'ailleurs, tous les modèles de campus cyber en France diffèrent les uns des autres.

Bien entendu, nous ne remettons nullement en question le bien-fondé du projet de loi. Nous y sommes favorables. Les collectivités territoriales ont déjà anticipé certains chantiers et ne partent donc pas de zéro.

Il faudra avant tout veiller à l'absence de surtransposition. Un réel problème d'accompagnement des collectivités se pose devant le coût de la mise en œuvre des nouvelles obligations. Enfin, rien ne sera possible aussi longtemps que n'interviendra pas une clarification de la stratégie de l'État en matière de cybersécurité, du rôle de l'Anssi, de la compétence, du portage politique et de la gouvernance de cette politique.

Jérôme Tré-Hardy, conseiller régional de Bretagne, représentant de Régions de France. – À mon tour, je vous remercie d'entendre les collectivités territoriales sur ce sujet extrêmement important de la transposition de la directive NIS 2.

Je prendrai l'exemple de la région Bretagne, la deuxième en importance après l'Île-de-France dans le domaine de la cybersécurité, marquée par la volonté politique de Jean-Yves Le Drian, en son temps, et par une forte présence militaire. Pour autant, l'humilité commande de reconnaître que les risques de cybersécurité n'y sont pas moindres que dans d'autres régions.

Il importe du reste de sensibiliser à la culture cyber et de la diffuser dans l'ensemble de la société. C'est pourquoi nous nous sommes emparés des campus cyber comme d'une possibilité de fédérer tout l'écosystème breton et de réunir toutes les parties prenantes, notamment sur la réflexion relative à la transposition de la directive européenne. Je précise que Régions de France

représente au sein du conseil d'administration du campus cyber l'ensemble des régions labellisées.

Le sujet des Csirt provoque nombre de commentaires et d'échanges. En Bretagne, le centre régional a fait la démonstration de sa pertinence : il a répondu à 115 incidents en 2024 et les maires qu'il a accompagnés se disent satisfaits du service rendu.

Le financement est un sujet clé, mais nous ne devons pas oublier ce qui a d'ores et déjà été réalisé.

Nous nous sommes intéressés aux conséquences de la transposition de la directive en Bretagne. La mise à niveau des systèmes d'information requerra vraisemblablement plusieurs millions d'euros. Au vu des contraintes budgétaires actuelles, avons-nous véritablement les moyens de notre ambition ? Telle est la question que nous devons collectivement nous poser, et elle s'étend à la dimension des ressources humaines.

Je vous ferai enfin part de deux convictions. D'une part, l'échelon régional ne doit pas être négligé, en raison de son aptitude à relier les politiques nationale et européenne ; d'autre part, la coopération, caractéristique de notre manière de travailler en Bretagne, prend toute son importance en la matière parce qu'elle favorise l'optimisation budgétaire et le partage des bonnes pratiques.

Mme Marlène Le Dieu de Ville, vice-présidente d'Intercommunalités de France chargée du numérique, vice-présidente déléguée à l'économie numérique, aux systèmes d'information et à la culture de la communauté de communes de Lacq-Orthez. – Au sein d'Intercommunalités de France, la perspective de la transposition de la directive NIS 2 nous tient à cœur. Il y a deux ans, les intercommunalités avaient lancé leur propre baromètre de maturité numérique, lequel avait révélé que la cybersécurité était la première de leurs priorités. Il faut dire que, entre 2022 et 2023, elles ont été, selon l'Anssi, victimes de 187 attaques. Et le rythme de ces dernières ne faiblit pas, quelle que soit au demeurant la taille des collectivités.

Nous avons particulièrement apprécié les consultations que l'Anssi a menées auprès des associations d'élus et avons beaucoup travaillé avec cet organisme, en réunissant notamment dans une commission numérique une cinquantaine d'intercommunalités allant de la communauté de communes de 5 000 habitants à la métropole de 1 million d'habitants. Et nous cernons désormais mieux les conséquences du projet de loi pour elles.

Toutes les intercommunalités sont finalement concernées par la directive NIS 2. Le seuil de 30 000 habitants nous semblait peu conforme à la réalité du terrain, notamment à celle des 992 communautés de communes. Celles-ci seront qualifiées d'« entités importantes », aux côtés des communautés d'agglomération, des communautés urbaines et des métropoles qui auront la qualité d'« entités essentielles ». Remarquons néanmoins que les

écarts sont en pratique notables dans chacune des deux catégories, par exemple au sein des communautés de communes entre celles qui comprennent quelque 5 000 habitants et celles qui en comprennent 70 000, ou entre une communauté d'agglomération de 30 000 à 50 000 habitants et une métropole de 1 million d'habitants. La transposition de la directive devra en tenir compte.

Avec l'Anssi, nous abordons déjà la phase réglementaire, qui suivra l'adoption du projet de loi. Nous allons ainsi constituer des groupes de travail, une première réunion étant prévue le 20 février prochain avec l'association Les Interconnectés. Y prendront part un petit nombre de métropoles, un nombre plus important de communautés d'agglomération et un nombre plus élevé encore de communautés de communes. L'objectif est que l'Anssi se forge une idée des conséquences des nouvelles obligations sur chacune des structures intercommunales et de leurs difficultés respectives. Il importe également de proposer des mesures adaptées à la réalité du terrain.

Intercommunalités de France joue un rôle de mutualisation entre les communes, auquel nous sommes très attachés. La directive NIS 2 et sa transposition nous donnent l'occasion d'accompagner les communes, à des degrés variables selon les situations. Le projet de loi doit nous fournir un cadre clair, simple et pratique, afin de nous permettre d'avancer dans la bonne direction.

En ce qui concerne les points de vigilance, je veux insister, comme mes collègues, sur la question de la proportionnalité. Pour l'instant, c'est un peu flou, on nous assure que les délais seront adaptés, mais nous ne savons pas comment. Nous avons, je le répète, à la fois de très petites et de grosses intercommunalités et cette proportionnalité, même pour les entités importantes, va imposer un certain nombre d'obligations, à commencer par le fait de transmettre des informations en cas d'attaque. Il faudra garantir que ce ne soit pas trop compliqué lorsque l'on aura la tête dans le guidon. L'Anssi affirme qu'il ne s'agira que de questionnaires simples à remplir, mais je demande à voir. Elle insiste beaucoup sur la simplicité, mais pour les entités essentielles, les choses restent floues ; par exemple, on nous assure qu'un RSSI ne sera pas requis, qu'un simple référent en cybersécurité suffira. Soit, mais je demande à voir. Peut-être que notre groupe de travail, qui se réunira une fois par mois jusqu'à la fin de la phase réglementaire, s'y penchera.

Il y aura en effet besoin d'un accompagnement financier et en ingénierie, à tous les niveaux ; nous n'avons pas évalué les besoins, mais nous le ferons en partenariat, je l'espère, avec l'Anssi. Je vais vous raconter une anecdote, pour bien mesurer les besoins d'accompagnement des collectivités les plus petites : au moment du plan France Relance, qui permettait aux collectivités de mettre en place une véritable politique de cybersécurité, ont profité de l'accompagnement proposé quasiment toutes les métropoles, 50 % des communautés d'agglomération et seulement 10 % des communautés de communes, c'est-à-dire les collectivités qui en avaient le plus besoin. La raison

en est simple : une condition pour être accompagné était d'avoir un DSI. Cela montre le faible niveau de maturité numérique des petites collectivités… En tout état de cause, cet accompagnement est crucial et il faudra le calibrer différemment selon les strates de collectivités, qui n'ont pas toutes les mêmes moyens.

Pour ce qui est du délai, les collectivités sont soumises aux règles des marchés publics ; aussi, pour remettre en cause certains contrats, il faudra du temps et le délai de trois ans pourrait être insuffisant. Certaines métropoles elles-mêmes, plus rompues que les communautés de communes à ce genre d'exercice, indiquent qu'il leur faudra certainement plus de trois ans pour remettre en cause certains marchés.

Par ailleurs, et cela concerne davantage les plus petits, qui y font plus appel, on va manquer cruellement de prestataires privés. On parle beaucoup de grands groupes, mais nous ne voulons pas tuer les entreprises locales ; nous avons une compétence développement économique et nous ne souhaitons pas que les grands groupes raflent tout, sans parler de la question du coût. Par conséquent, un problème de prestataires risque de se poser, d'autant que nous ne pourrons pas être garants de la cybersécurité des outils qui nous seront proposés, nous n'en sommes pas capables. On nous a signalé que des prestataires seront certifiés, par exemple par l'Anssi ; si c'est le cas, tant mieux. Je sais le travail colossal réalisé par les campus cyber et les entreprises pour monter en compétence dans ce domaine, et je salue ce travail. J'espère que cela sera bien pris en compte par l'État.

En matière de ressources humaines, nous aurons des difficultés de recrutement, surtout pour les petites collectivités. On a besoin de visibilité, au niveau tant national que régional ; on doit pouvoir s'assurer que les acteurs locaux seront encore là dans un an ou deux, et que l'on pourra toujours travailler avec eux. La visibilité à l'échelon interministériel et au sein des associations d'élus n'est pas évidente ; il n'est pas simple de parler avec l'État, car plusieurs ministères sont parfois impliqués. Enfin, nous souhaiterions avoir une meilleure communication institutionnelle de l'État à destination de l'ensemble des acteurs.

M. Geoffroy Boulard, maire du XVII^e^ arrondissement de Paris, conseiller de Paris, vice-président de la métropole du Grand Paris. – La métropole du Grand Paris réunit 130 communes, couvre 11 territoires sur 3 départements – Hauts-de-Seine, Seine-Saint-Denis, Val-de-Marne – sans compter Paris et quelques communes limitrophes de l'Essonne et du Val-d'Oise.

La métropole est compétente pour piloter différents enjeux liés à l'environnement, à l'attractivité, à l'énergie, à l'habitat ou encore à l'aménagement. Face à ces défis, la métropole du Grand Paris a souhaité construire un écosystème favorable à l'innovation, *via* notamment des dispositifs consacrés à l'innovation et au numérique.

Elle a en outre créé des programmes d'accompagnement des communes, en matière de data ou de numérique. Par exemple, elle met en œuvre des programmes d'accompagnement et de cofinancement d'expérimentations de solutions innovantes ou numériques, tels que Innover dans la ville ou Quartiers métropolitains d'innovation, mais aussi des réseaux d'acculturation aux enjeux numériques et d'innovation, avec des académies de formation comme le Réseau des explorateurs, destiné aux agents des différentes communes, et un réseau d'élus. La métropole du Grand Paris réfléchit également à une stratégie sur l'intelligence artificielle, qui sera présentée en avril au conseil métropolitain.

Le développement du numérique et l'innovation sont source d'opportunités, mais la métropole reste naturellement vigilante à leurs effets sur la maîtrise inégale des compétences numériques, l'environnement ou l'apparition de nouvelles dépendances et fragilités. D'où le besoin de renforcer la cybersécurité. C'est pourquoi nous avons adopté dès 2019, dans le schéma métropolitain d'aménagement numérique, le principe d'un soutien prioritaire de la gestion de la sécurisation des données publiques.

L'étude de 2024 de *cybermalveillance.gouv.fr* montre qu'une collectivité sur dix déclare avoir été victime d'une ou plusieurs attaques au cours de l'année dernière, que l'hameçonnage est la cause principale dans 30 % des cas, que 45 % des collectivités attaquées n'en connaissent pas la cause et que les collectivités touchées ont principalement déploré une interruption de service, mais aussi une destruction ou un vol de données, ou encore une perte financière. Toujours d'après cette étude, 44 % de ces communes s'estiment faiblement exposées au risque et 18 % des communes ne savent pas évaluer le risque. Ce chiffre s'explique, selon moi, par le fait que, ne se pensant pas vulnérables, elles surestiment l'efficacité de leur système de protection et sont insuffisamment préparées aux cyberattaques.

La fracture se creuse entre les communes. Il y a des dispositifs d'aide en faveur de la cybersécurité, comme France Relance ou encore MonAideCyber, mais il reste un manque de connaissances et d'accompagnement des petites communes, en moyens humains et financiers. L'étude signale d'ailleurs qu'il n'y aura pas d'évolution majeure des budgets consacrés à l'informatique et à la sécurité des systèmes d'une année sur l'autre et que 73 % des petites et moyennes collectivités ont un budget informatique annuel de moins de 5 000 euros, les deux tiers d'entre elles n'envisageant pas d'évolution à la hausse, alors qu'elles sont fortement exposées au risque.

Les éléments statistiques identifiés à l'échelle nationale par l'étude se retrouvent au sein du territoire de la métropole du Grand Paris. Nous avons toujours souhaité que cette collectivité soit une métropole des maires et, lors des rencontres avec les communes, il est apparu que la question de la cybersécurité constituait un élément d'inquiétude majeure chez les maires, en particulier dans les communes disposant de peu de moyens ou d'un système d'information daté et peu développé.

J'ai échangé avec des maires ayant vécu ce type d'attaques et l'impact d'une cyberattaque sur une commune s'avère encore peu maîtrisé. Les agents doivent passer immédiatement en mode gestion de crise ; les communes connaissent ce type de situation, mais elles peuvent être prises au dépourvu lors d'une cyberattaque, car toutes leurs activités sont désorganisées, ce qui perturbe d'autant leur capacité de réaction. Pendant plusieurs jours, la majorité des agents ne peut plus travailler, dans l'attente de la restauration des systèmes d'information, et cette dernière se fait d'ailleurs étape par étape et non en bloc. Il est donc nécessaire de prendre en compte cette remise en marche progressive.

La cyberattaque a également des conséquences pour les usagers : suspension des inscriptions et des paiements à la cantine, versement des allocations des centres d'actions sociales, etc. L'équipe politique, notamment le maire, est alors en première ligne. Une cyberattaque entraîne aussi des répercussions à long terme : certaines villes ont mis entre deux et quatre années pour s'en remettre et pour remettre à jour certaines données de paiement. Les cyberattaques sont aussi éprouvantes pour les agents qui les ont vécues, elles entraînent une fatigue importante et un éventuel turnover.

Quelques exemples de cyberattaques contre les communes de la métropole du Grand Paris : en 2020, Bondy, Le Blanc-Mesnil, Vincennes ; en 2021, Tremblay-en-France, Villepinte, Bobigny, La Courneuve ; en 2022, Saint-Cloud, Chaville ; en 2023, Bry-sur-Marne et Chevilly-Larue.

La transposition de NIS 2 est l'occasion de s'interroger sur la place des collectivités dans ce dispositif. L'Anssi a déclaré le 3 septembre dernier que les collectivités devaient se saisir de cette opportunité face à la menace, mais les dispositifs de NIS 2 n'intégreront peut-être pas toutes les collectivités, ils pourraient n'en cibler que certaines, en fonction de leur taille. Il convient de s'assurer que les collectivités visées disposeront des moyens humains et financiers pour mettre en œuvre les exigences de sécurité de la directive. Or, d'après l'étude de *cybermalveillance.gouv.fr*, 62 % des collectivités demandent une sensibilisation accrue des élus et des agents. La mise en place d'outils de sécurisation est privilégiée et l'accompagnement financier des territoires est au cœur des attentes.

La métropole du Grand Paris a institué un accompagnement de ses communes, sans attendre le projet de loi de transposition, pour être aussi conforme que possible à ces directives. Elle est donc engagée depuis 2021 *via* un programme européen, le projet Cybiah (Cybersécurité et intelligence artificielle hub), lauréat du programme Edih (*European Digital Innovative Hub*). Le campus cyber d'Île-de-France a rassemblé des entreprises, des associations et des acteurs publics, afin de proposer la création d'un Edih consacré à la cybersécurité. Ce projet vise à créer tout simplement un guichet unique permettant de développer des actions en faveur de cybersécurité auprès des TPE et PME et des collectivités territoriales sur le territoire francilien.

Pour sensibiliser ces acteurs à la mise en œuvre d'une stratégie cyber adaptée à leurs besoins, Cybiah a construit un parcours d'accompagnement des TPE divisé en quatre phases : embarquement, diagnostic, sécurisation et cofinancement. Dans le cadre du projet Cybiah, la métropole du Grand Paris s'est positionnée, conjointement avec le campus cyber, pour décliner ce parcours d'accompagnement auprès des communes métropolitaines. Ce projet est mis en œuvre avec le soutien financier de la Commission européenne pour ce qui concerne les TPE et PME et les collectivités, et de la région Île-de-France pour ce qui concerne les TPE et PME.

Nous avons décliné ce programme auprès des communes métropolitaines. La première brique, 100 % gratuite pour les communes, permettra de formuler un diagnostic individualisé par commune évaluant le niveau de maturité en cybersécurité et d'élaborer un plan de sécurisation adapté aux besoins. Dans un deuxième temps, nous pourrons proposer un soutien financier pour la mise en place du plan de sécurisation, à hauteur de 50 % du coût du projet, dans la limite de 200 000 euros, grâce au fonds métropolitain Innover dans la ville. La troisième brique consiste à amener toutes les communes à un niveau satisfaisant en matière de cybersécurité. Nous avons ciblé les 30 communes, parmi les 130, qui ont le plus besoin de ce dispositif.

Nous avons également souhaité conduire une préanalyse en matière de cybersécurité des communes. Les résultats pourront servir à convaincre les communes d'entrer dans la démarche, car c'est parfois nécessaire – d'ailleurs, cette évaluation externe n'aura pas d'impact sur le fonctionnement des services –, et ils seront communiqués.

Nous avons lancé le 23 janvier dernier ce programme. Déjà dix communes ont demandé à en bénéficier et, vendredi prochain, nous organisons un événement au campus cyber.

M. Olivier Cadic, président. – Je remercie chacun de vous pour son investissement et merci d'avoir cité *cybermalveillance.gouv.fr*, acteur essentiel de la cyberprotection des entreprises et des particuliers. Je salue le lancement de la plateforme 17Cyber au mois de décembre dernier.

M. Patrick Chaize, rapporteur. – Je concentrerai mon intervention sur la transposition de la directive NIS 2. Avec cette directive, il s'agit non plus seulement de sécuriser des infrastructures critiques, mais aussi d'assurer la résilience des entités critiques en tant qu'organisations et de l'ensemble de leurs systèmes d'information. Cette résilience est indispensable pour les collectivités territoriales, car celles-ci sont de plus en plus victimes de cyberattaques, avec 187 incidents concernant traités par l'Anssi entre janvier 2022 et juin 2023.

Alors que l'imposition des règles aux collectivités est laissée au libre choix des États membres dans la directive, la France a fait le choix de les intégrer dans ces nouvelles exigences, au regard de la multiplication des

attaques affectant les services publics locaux et leur faible sécurisation. Le projet de loi prévoit ainsi que 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 300 communes de plus de 30 000 habitants, devront se conformer au corpus législatif résultant de la transposition de la directive NIS 2. En particulier, chacune de ces collectivités devra évaluer si elle est soumise à la directive, si elle est entité essentielle ou entité importante et si elle doit s'enregistrer auprès de l'Anssi et lui notifier tout incident de cybersécurité.

Partagez-vous le constat selon lequel les collectivités territoriales sont souvent vulnérables face aux menaces cyber ? Beaucoup d'entre elles se disent inquiètes, considèrent ce sujet comme très important, mais peu sont armées pour y faire face et envisagent les évolutions budgétaires nécessaires ; c'est-ce pas incohérent ? Comment corriger cette incohérence ?

Considérez-vous que les obligations mises à la charge des collectivités sont adaptées aux moyens et à la maturité des acteurs ? Pensez-vous que les collectivités sont suffisamment informées des changements à venir ? Seront-elles en mesure de s'y conformer rapidement et comment faire évoluer leur niveau d'information ?

Enfin, l'Anssi vous paraît-elle bien identifiée par les collectivités territoriales comme un interlocuteur de confiance dans le domaine de la cybersécurité ? Les entités régulées par la directive NIS 2 devront s'enregistrer auprès de cette agence et lui signaler tous les incidents significatifs de cybersécurité.

M. Hugues Saury, rapporteur. – Quel bilan tirez-vous du dispositif actuel de sécurité des activités d'importance vitale pour les collectivités territoriales ? Certains ont donné des statistiques, mais je voudrais savoir quelle est la proportion d'adhérents que vous considérez comme robustes en matière de défense cyber, au sein de chacune de vos organisations.

Comment évaluez-vous la philosophie générale de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) et du titre Ier du projet de loi, notamment sur la priorité donnée à la résilience par rapport à la protection ? Quel regard portez-vous sur les définitions de l'activité d'importance vitale, de l'infrastructure critique, du point d'importance vitale et système d'information d'importance vitale ? Les obligations prévues – plan de résilience opérateur et particulier, notifications d'incident, exigence spécifique pour les entités critiques européennes – vous semblent-elles pertinentes et proportionnées ? Comment jugez-vous les mécanismes de contrôle, d'astreinte et de sanction prévus en cas d'obstruction ?

Le Conseil national d'évaluation des normes (CNEN) a émis un avis défavorable sur ce projet de loi, au regard de la non-compensation des coûts

qu'il engendrera ? Quelles mesures l'État pourrait-il prendre pour accompagner les collectivités, leurs groupements ou leurs établissements qui seront des opérateurs d'importance vitale ?

M. Michel Canévet, rapporteur. – Selon vous, ce projet de loi surtranspose-t-il la directive NIS 2 en matière d'obligations pesant sur les collectivités territoriales ?

Faut-il allonger le délai de mise en œuvre de ces obligations ?

M. Mickaël Vallet. – Pour éviter de réinventer l'eau chaude, ne serait-il pas opportun d'intégrer un volet numérique dans les plans de crise des communes et intercommunalités, conformément d'ailleurs à une recommandation de l'AMF de novembre 2020 ? Cela pourrait-il constituer une piste pour les quelque 21 000 communes tenues de rédiger un plan communal de sauvegarde (PCS) ?

Mme Catherine Morin-Desailly. – La transposition de ce texte met en lumière les carences de l'État dans son rôle de stratège. Aucun des quatre ministres du numérique qui se sont succédé en peu de temps n'avait de vision transversale du sujet. Nous militons depuis dix ans pour la création d'un haut-commissariat au numérique.

Les collectivités se sentent-elles assez accompagnées et éclairées pour se prémunir contre les cyberattaques menées sur les infrastructures physiques, sur les logiciels, les *data centers ?* Sur le choix de logiciels, de quel éclairage bénéficiez-vous sur la protection des données à protéger ? Vous sentez-vous accompagnées par l'Anssi et la Commission nationale de l'informatique et des libertés (Cnil) ?

Les cyberattaques concernent les collectivités, mais également les établissements de santé et les établissements scolaires, de tous niveaux. Il y a des choix technologiques à faire quand on équipe les établissements, en matière de matériel et de logiciels. Comment cela se passe-t-il avec l'éducation nationale ? Le personnel vous semble-t-il formé et compétent ?

M. Ludovic Haye. – Je veux parler de la politique de gestion du risque. On ne peut pas demander aux collectivités, au travers de ce projet de loi, plus que le prix d'une éventuelle attaque. Une politique nationale efficace ne doit pas empêcher une articulation agile à l'échelon territorial, car aucune collectivité ne ressemble à une autre, sur la forme comme sur le fond, donc leurs besoins diffèrent. Cette directive ne doit pas constituer une épée de Damoclès supplémentaire au-dessus de la tête des communes.

Prévoir un coefficient de proportionnalité entre l'argent investi et le niveau de sécurité atteint est utopique. On peut se protéger de manière efficace sans investir trop. Ne nous lançons pas dans une fuite en avant.

Par ailleurs, ce qui paraît être un investissement peut se transformer en dépense de fonctionnement au fil du temps.

Les actions de bon sens au sein des communes consistent parfois simplement à identifier ses données critiques et à définir une politique de restauration en cas de problème.

Du point de vue des ressources humaines, nombre de communes n'auront jamais les moyens de s'offrir les services d'un spécialiste du cyber ; elles n'ont déjà pas les moyens de payer une secrétaire à plein temps. La solution pourrait être de tout transférer à l'EPCI mais il ne faut pas créer de fracture numérique supplémentaire.

Mme Audrey Linkenheld. – J'ai subi une cyberattaque d'ampleur à Lille, en tant que première adjointe. Je mesure ce que cela implique.

Pourriez-vous revenir sur la différence entre le niveau régional et national de l'Anssi pour l'accompagnement ? Et qu'en est-il de la Cnil, interlocuteur national, dont on a besoin quand on est victime d'une cyberattaque ?

Comment voyez-vous l'articulation entre la compétence numérique, la compétence économique et la compétence cyber entre les différentes strates territoriales ?

Je suis moi aussi favorable à l'intégration d'un volet cyber au sein des PCS, car cela s'avère toujours utile quand on doit tout redémarrer après une attaque. Au-delà des aspects numériques de la continuité et la reprise de l'activité, considérez-vous qu'il y a un déficit d'accompagnement de l'État sur les processus ? Quand on n'a plus de système informatique, comment délivre-t-on un acte d'état civil ou un permis de construire, bref comment assure-t-on la continuité du service public ?

Mme Vanina Paoli-Gagin. – Gagnerait-on à orienter la commande publique des collectivités vers des outils moins vulnérables, en *open source* et d'origine européenne ?

Sur les ressources humaines, le département de l'Aube a créé une université qui forme à la sécurité globale et un institut qui propose des formations en la matière.

Sur le financement, avez-vous, chacun à son niveau, des discussions avec France Assureurs ? La cyberattaque est un risque et, quand il y a un risque, on se tourne vers les compagnies d'assurance.

M. Michel Sauvade. – L'AMF et Départements de France sont des associations généralistes, elles sont soutenues par l'expertise d'associations plus spécialisées. Dans le domaine du numérique, on compte sur l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (Avicca) et sur la Fédération nationale des collectivités concédantes et régies (FNCCR).

Je partage les interrogations de M. Chaize sur la vulnérabilité des collectivités, qui est vraie dans d'autres domaines de sécurité d'ailleurs,

comme la voirie. M. Chaize a raison, il y a une incohérence : l'AMF est consciente que les élus locaux doivent assumer leurs responsabilités et, ce qui fait défaut, c'est le portage politique, qui n'est pas pleinement assuré par les collectivités. Il l'est sans doute plus au niveau des départements, parce que les moyens sont supérieurs. Il y a un déficit de notre part de portage politique sur un sujet perçu comme très technologique et peu intéressant. La position de l'AMF est claire : s'il y a un sujet politique, c'est bien celui du numérique.

Or les budgets ne sont pas proportionnés. L'information des collectivités n'est pas suffisante non plus, mais c'est aussi à nous de faire l'effort de nous informer. Sommes-nous en mesure de nous y conformer rapidement ? Certainement pas. L'Anssi est-elle identifiée par les collectivités ? Je ne le pense pas.

Monsieur Saury, je ne sais pas vous dire quelle proportion de nos adhérents semble robuste. Toutes les collectivités me semblent fragiles, mais je n'ai pas de statistique. Les budgets des départements sont sinistrés, mais je n'ai pas d'information précise sur le numérique. Je comprends la difficulté sur la proportionnalité des mécanismes de contrôle et l'avis défavorable du CNEN.

Monsieur Canévet, certains points paraissent curieusement sous-transposés, comme l'identification des incidents à faire remonter, et d'autres posent problème. La question des délais va se poser, mais la question est surtout notre capacité à travailler ensemble pour que les délais soient adaptés.

Monsieur Vallet, il y a l'unité cyber de la gendarmerie nationale, qui permet aux collectivités de s'identifier en cochant 10 cases, avec un accompagnement local qui permet aux plus petites communes de mettre un point d'attention sur les difficultés majeures. L'AMF se veut le relais de l'ensemble des collectivités.

Madame Morin-Desailly, les collectivités ne sont pas assez accompagnées. Nous voulons faire du numérique un sujet à part entière, plutôt que de l'inclure dans le PCS. Pour moi, c'est spécifique.

Monsieur Haye, sur la politique de gestion du risque, je suis d'accord, il ne faut pas demander plus que le prix de l'attaque. Une réponse peut venir de l'État, s'il parvient à créer une dynamique collective. L'État pèche par défaut d'engagement.

Madame Paoli-Gagin, pour une collectivité qui ne dispose pas de capacités de suivi et de mise à niveau, le recours à l'*open source* ou à des produits européens n'est pas vraiment la question. Dans le Puy-de-Dôme, je n'avance pas vers plus de numérique et de cybersécurité, j'essaie déjà de me débrouiller pour résorber la dette numérique creusée par l'absence d'une politique globale adaptée.

Mme Constance Nebbula. – Je commence par la question de la prise de conscience. À l'échelle des régions, il serait faux d'affirmer qu'il n'y en a

pas, il s'agit tout de même de collectivités fortes, avec de grosses DSI et des moyens. En revanche, le niveau inférieur n'a pas eu cette prise de conscience. Je vous l'ai dit, 23 % de ces collectivités n'ont jamais entendu parler de NIS 2 et je vais illustrer mon propos d'une anecdote. La région des Pays de la Loire a un groupement d'intérêt public qui accompagne la transformation numérique des collectivités. La base de la base, c'est d'avoir une adresse électronique sécurisée. Or, quand nous proposons gratuitement aux petites communes d'avoir un nom de domaine propre et de l'héberger, en remplacement de l'adresse utilisée, nombre de maires refusent et préfèrent garder leur adresse Gmail. La prise de conscience n'existe pas dans les strates plus petites.

En ce qui concerne l'Anssi, heureusement qu'on l'a en région ! En revanche, l'Anssi en région manque de moyens pour nous aider. Je suis élue à Angers ; cette ville a été victime d'une cyberattaque il y a trois ans et demi et a mis trois ans pour s'en remettre. Notre premier réflexe, après l'attaque, a été de contacter l'Anssi. Qui nous a aidés ? L'Anssi et le secteur privé. On est un peu en mode « débrouille », mais heureusement qu'on a l'Anssi et c'est l'Anssi en région qu'il faut renforcer.

En revanche, on n'a pas beaucoup de liens avec la Cnil, ce n'est pas une agence décentralisée, ce n'est pas un interlocuteur local, ce n'est pas un partenaire pour les élus.

En ce qui concerne les sanctions, monsieur le président, vous avez déclaré un jour, à une table ronde où j'étais aussi, que la loi est la même pour tout le monde. Je suis d'accord sur le principe, à condition qu'il y ait l'accompagnement nécessaire. Soit il y a une différence entre le secteur public et le secteur privé et les sanctions ne sont pas les mêmes, soit on décide de consacrer des moyens à l'accompagnement et alors les sanctions doivent être les mêmes. La sanction n'a aucun intérêt en elle-même et, je le répète, les collectivités croulent sous les sanctions, les réglementations, les normes. Commençons par accompagner avant de penser à sanctionner.

Pour ce qui est de la surtransposition, le sujet vient de l'Europe ; plus il y a de normes européennes, plus elles se déclinent à l'échelle locale, mais c'est un autre sujet.

Le délai de trois ans suffira pour les régions, car elles n'ont pas attendu pour commencer le travail.

Quelle place pour la transversalité ministérielle ? Question éminemment politique. À qui parle-t-on ? À Bercy, à l'intérieur ou à la défense ? On ne sait pas. Pour ma part, je défends depuis des années l'existence d'un ministre unique, du numérique, du cyber et de l'IA, qui dépend du Premier ministre, pour assurer la transversalité entre ministères. Sans cela, on ne pourra pas avoir de véritable stratégie de l'État.

M. Patrick Chaize, rapporteur. – Cela a existé !

Mme Constance Nebbula. – Oui, et c'était très bien.

Je suis présidente d'Open Data France, donc la question des données me touche particulièrement ; heureusement que des structures existent pour remédier aux manquements de l'État.

Les environnements numériques de travail dans les lycées sont attaqués. Dans les Pays de la Loire, un lycée a subi un piratage et des vidéos d'une violence inouïe ont été postées sur l'ENT ; le personnel n'est absolument pas formé à cela. Je ne sais pas comment répondre à cette question, je ne sais pas comment sensibiliser le personnel des établissements, puisque tout est numérisé.

En ce qui concerne le budget de fonctionnement des systèmes d'information, je vous confirme que, plus les années passent, plus les dépenses de fonctionnement augmentent ; c'est le seul budget des collectivités dans ce cas, puisque nous sommes censés réduire nos dépenses de fonctionnement et avoir plus d'investissements. C'est un problème.

Je termine avec la question des compétences. Le sujet est moins la compétence que la clarté : que l'on nous dise si, oui ou non, nous nous en occupons et, si nous nous en occupons, que l'on nous donne les moyens de le faire. Pour moi, le 17Cyber suscite une confusion, car c'est un numéro national : que faisons-nous des numéros régionaux ? Que faisons-nous des Csirt territoriaux ? Pour le grand public, les associations, les entreprises, quelle confusion ! Plus il y a d'organismes, moins on sait vers qui se tourner. Bref, nous sommes en mode débrouille…

M. Olivier Cadic, président. – C'est bien d'avoir un numéro unique, car toutes les régions n'ont pas un Csirt et c'est toujours mieux d'avoir un seul numéro valable sur tout le territoire et qui répartit les appels vers le bon interlocuteur.

M. Jérôme Tré-Hardy. – Je rappelle qu'il y a un lien entre les Csirt régionaux et le 17Cyber, en tout cas le travail de collaboration a été mené en Bretagne.

Je prône moi aussi le portage politique unique, mais nous avons, en Bretagne, une relation très proche avec le ministère des armées et je me suis rendu compte que le cyber a une dimension duale, comme l'IA : il y a un cyber civil et un cyber de défense. Or je ne suis pas certain qu'il soit si évident d'en faire un sujet transversal ; je pensais que cela allait de soi, mais plus j'approfondis cette question et plus elle me paraît complexe. Cela explique peut-être pourquoi nous avons du mal à avoir un portage unique.

Je suis intimement convaincu qu'il est indispensable de promouvoir une véritable montée en compréhension du risque cyber, à tous les niveaux. Sans doute, les régions se sont emparées du sujet et elles ont des moyens financiers importants, mais mes collègues élus sont encore bien éloignés de

ces sujets. Il faut donc adopter une posture d'humilité et faire monter en compréhension ce risque cyber.

Je souligne moi aussi le rôle primordial de l'Anssi dans les territoires, mais on lui fait porter beaucoup de choses sur les épaules, on a l'impression qu'elle va tout faire. Certains pensent, je le sais, que les Csirt ne servent à rien. Je pense le contraire : cela peut être une partie de la solution, parce que cela nous permet d'avoir un lien avec l'Anssi et avec les territoires, et de sensibiliser au risque cyber. La transposition de NIS 2 et l'examen de ce projet de loi sont l'occasion de parler du sujet.

La question des solutions souveraines est un vrai sujet, mais ce qui me trouble, c'est la dichotomie entre nos grandes ambitions en la matière et la réalité du terrain, quand on doit choisir certaines solutions : c'est plus facile, on est embarqué dans un type de relations, etc. Mais je suis d'accord avec vous. La sensibilisation des élus est extrêmement importante à ce sujet.

M. Olivier Cadic, président. – Et il faut avoir les moyens de ses ambitions…

Mme Marlène Le Dieu de Ville. – Les collectivités connaissent-elles l'Anssi et la Cnil ? Cela dépend de leur taille, mais est-ce gênant si elles ne les connaissent pas ? Pas forcément. Une commune peut facilement s'adresser à la gendarmerie nationale, qui est très à l'écoute et qui peut suffire. Ce n'est pas toujours la peine d'aller plus loin.

Sur la gestion des risques, je suis d'accord, il n'est pas toujours nécessaire de dépenser des sommes importantes dans des équipements, il suffit parfois d'avoir de bonnes pratiques. Le diagnostic peut être fait par MonAideCyber ou par la gendarmerie. Dans ma commune, j'ai fait mon diagnostic avec MonAideCyber et il s'agit de questions simples. De grosses dépenses ne sont pas toujours requises, en tout cas dans les petites collectivités.

En revanche, l'accompagnement est proche de zéro, chacun se débrouille comme il le peut. Les intercommunalités tâchent d'accompagner leurs communes, sans avoir la compétence ; elles ne tiennent d'ailleurs pas vraiment à l'avoir. Simplement, elles essaient de mutualiser les volontés et les moyens. Et il ne faudrait pas que les obligations soient trop complexes.

En ce qui concerne la gestion des risques, il me paraîtrait intéressant d'ajouter, dans les plans communaux ou intercommunaux de sauvegarde, un volet cyber et un protocole à mettre en place en cas de crise. Cela peut être des choses très basiques, quelques interlocuteurs, car les petites intercommunalités ont peur mais sont perdues face à la réponse. Et il faudrait aussi prévoir un plan pour la suite de l'attaque : une fois la crise gérée, comment reprend-on son activité ?

M. Geoffroy Boulard. – Le portage politique manque, c'est vrai. On a cité certains ministères, mais on a oublié les ministères des comptes publics et

de la fonction publique. On a saucissonné le numérique depuis une dizaine d'années, ce qui entraîne un manque d'impulsion politique. Les enjeux d'intelligence artificielle exigent un ministère de plein exercice et régalien.

L'accompagnement de l'État et de l'Anssi est-il suffisant ? L'Anssi joue son rôle, on a des retours positifs sur son action en situation de crise. Ensuite, il faut restaurer les données, ce qui pose la question du rôle régalien de l'État en matière de souveraineté numérique.

Les collectivités n'ont pas de budget sur ce sujet. Elles doivent déjà mettre à niveau leurs systèmes d'information. C'est pour cela que nous proposons un accompagnement gratuit, afin que les communes acceptent d'être accompagnées, mais ensuite, elles doivent s'y investir. Nous avons la chance de pouvoir donner une impulsion politique, mais nous avons fait un choix. Par ailleurs, nous finançons des projets jusqu'à 50 %, mais encore faut-il pouvoir compléter.

L'acculturation progresse, les réseaux d'élus se forment et il y a une volonté d'appréhender le sujet.

On peut parler de surtransposition. Les collectivités se débrouillent, mais, attention, on va ajouter de nouvelles contraintes, les collectivités risquent d'être sanctionnées, alors que l'État ne les a jamais accompagnées à la hauteur des enjeux. Il y a urgence, soit, mais il y a aussi urgence à définir une stratégie, pour définir ce qui relève de l'État, des collectivités, du privé, avec le sujet de la souveraineté. Et il y a aussi la question de la filière : les DSI de communes, même robustes, ont des difficultés à trouver des prestataires qualifiés, à même de les accompagner. On a parfois peu le choix entre les solutions techniques.

Le contrôle, la sanction, ce n'est pas notre enjeu. Notre enjeu est de poursuivre l'évangélisation des communes. Avec une couche supplémentaire de sanctions, le numérique punitif aura des conséquences néfastes et aggravera les inégalités.

M. Olivier Cadic, président. – Merci. Vous avez bien exposé vos préoccupations. Cette table ronde était très instructive.

M. Patrick Chaize, rapporteur. – Je comprends que les dépenses de fonctionnement augmentent, mais ne s'agit-il pas d'une dépense d'investissement détournée ?

M. Olivier Cadic, président. – Quand on investit 100 pour une application, on doit en effet prévoir 7 à 10 pour la maintenance.

M. Geoffroy Boulard. – Selon l'interprétation de la commune, les mêmes dépenses peuvent être enregistrées en section de fonctionnement ou d'investissement. C'est un véritable problème.

M. Olivier Cadic, président. – Merci de tous ces éléments.

MARDI 11 FÉVRIER 2025

1. Les autorités de régulation financière - Audition de l'Autorité des marchés financiers et de l'Autorité de contrôle prudentiel et de résolution

M. Olivier Cadic, président. – Notre cycle d'auditions publiques consacrées au projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité se poursuit aujourd'hui par une première table ronde avec les autorités de régulation financière.

L'Autorité des marchés financiers (AMF) est ici représentée par M. Sébastien Raspiller, secrétaire général, qui est accompagné de M. Philippe Sourlas, secrétaire général adjoint en charge de la direction de la gestion d'actifs, et de Mme Laure Tertrais, directrice de cabinet auprès de la présidente Mme Marie-Anne Barbat-Layani.

M. Frédéric Hervo s'exprimera en sa qualité de secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR) ; il est accompagné de Mme Véronique Bensaid-Cohen, conseillère parlementaire auprès du Gouverneur, de M. Alexandre Garcia, expert en régulation prudentielle bancaire et politique de stabilité financière, et de M. Gabriel Preguiça, chargé de mission.

Je vous remercie d'avoir répondu à notre invitation, car vous pourrez ainsi nous éclairer sur le dernier des trois volets de ce projet de loi, à savoir la transposition de la directive qui concerne la résilience opérationnelle numérique du secteur financier, dite « DORA ». Ce titre III entre dans le champ de compétences de notre collègue corapporteur Michel Canévet, par ailleurs membre de la commission des finances.

Nos auditions avaient jusqu'à présent surtout porté sur les deux premiers titres du projet de loi, lesquels concernent respectivement la transposition de la directive sur la résilience des entités critiques, dite « REC », et la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS2 ». Pour autant, ces sujets ne sont pas sans lien puisque certaines questions ont été soulevées lors de précédentes auditions sur les recoupements ou redondances pouvant exister entre ces trois directives. Mes collègues corapporteurs sur les titres I et II, respectivement Hugues Saury et Patrick Chaize pourront vous demander des précisions à ce sujet.

Avant de vous céder la parole, je vous rappelle que cette audition fait l'objet d'une captation vidéo qui est retransmise sur le site internet du Sénat puis consultable en vidéo à la demande.

Je propose que les rapporteurs posent d'emblée leurs questions pour que vous puissiez y répondre dans votre propos liminaire, ce qui laissera plus de temps ensuite pour la séquence de questions-réponses.

M. Michel Canévet, rapporteur. – Pouvez-vous nous indiquer les principaux risques que vous avez identifiés concernant le secteur financier en matière de cyber. Un certain nombre de normes n'ont pas encore été publiées. Ne pensez-vous pas que ces normes sont trop précises, ce qui entraîne des contraintes supplémentaires pour l'ensemble des institutions financières et des coûts administratifs pour l'ensemble des acteurs, c'est-à-dire non seulement les entreprises, mais aussi les superviseurs ?

J'aborderai trois sujets de préoccupation.

Premièrement, plusieurs directives ou règlements sont inclus dans le projet de loi Résilience. Les entreprises, notamment du secteur financier, pourraient être soumises à la fois aux obligations prévues par la directive NIS2 et la directive DORA. Comment éviter une telle complexification ?

Deuxièmement, les sociétés de financement ne sont pas incluses dans la directive DORA. Est-il pertinent de les inclure, comme le propose la France ? Certes, un délai supplémentaire est accordé à ces sociétés, jusqu'en janvier 2026 ? Est-ce suffisant ? Ne faudrait-il pas adopter une approche plus proportionnée ?

Troisièmement, enfin, j'évoquerai la question du reporting des incidents, qui sous-tend une adaptation des superviseurs. L'Agence nationale de la sécurité des systèmes d'information (Anssi) est organisée pour pouvoir fonctionner vingt-quatre heures sur vingt-quatre. Comment l'ACPR et l'AMF entendent-elles modifier leur organisation interne pour assurer la continuité du reporting ?

M. Patrick Chaize, rapporteur. – Je suis plus particulièrement chargé du titre II consacré à la transposition de la directive NIS2. Si cette audition est consacrée à la directive DORA, les infrastructures du marché financier et le secteur bancaire sont également concernés par la directive NIS2 en tant que secteurs hautement critiques.

Avec cette directive, c'est un changement majeur de paradigme qui est à l'œuvre : il ne s'agit plus seulement de sécuriser des infrastructures critiques, mais d'assurer la résilience des entités critiques. Les entreprises des secteurs bancaire et financier sont-elles suffisamment informées des changements à venir ? Pensez-vous que l'Anssi est suffisamment bien identifiée par le monde financier comme un « interlocuteur de confiance » dans le domaine de la cybersécurité ? Enfin, l'articulation des dispositions prévues dans les directives NIS2 et DORA, et dans le cadre du projet de loi qui les transpose, entre ses titres II et III, vous paraît-elle adéquate ? Avez-vous, le cas échéant, identifié des difficultés ?

M. Frédéric Hervo, secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution. – Je suis très honoré d'échanger avec vous sur la mise en œuvre du règlement DORA relatif à la résilience informatique et cyber du secteur financier, qui fait l'objet, comme vous l'avez rappelé, d'un titre spécifique du projet de loi Résilience. En tant que secrétaire

général adjoint de l'ACPR, l'autorité chargée du contrôle des secteurs bancaire et de l'assurance, je peux vous confirmer que ce sujet nous mobilise fortement en ce qu'il est essentiel pour la stabilité financière en France, mais aussi au sein de l'Union européenne.

Le contexte dans lequel s'inscrit cette nouvelle réglementation est marqué par deux éléments essentiels.

D'une part, nous vivons une digitalisation accélérée du secteur financier. En tant qu'utilisateurs de services bancaires et financiers, nous le vivons tous au quotidien. En tant que superviseurs, nous avons constaté au cours des dernières années l'essor de services supports de plus en plus massifs et complexes, tels les *clouds* ou les centres de données importants, y compris s'agissant des domaines liés à l'intelligence artificielle. Ces services sont proposés aux établissements financiers par des géants du numérique, dont beaucoup sont basés en dehors de l'Union européenne, ce qui soulève évidemment un certain nombre de questions sur la performance, la réussite de la transformation digitale et, bien sûr, les risques qui y sont associés.

D'autre part, nous constatons l'essor des cyberattaques à l'encontre du secteur financier, l'un des secteurs les plus affectés. Pour rappel, en 2024, la filiale américaine de la banque chinoise ICBC a dû être recapitalisée à hauteur de plusieurs milliards de dollars à la suite d'une cyberattaque au moyen d'un rançongiciel. Dans le cadre de son évaluation des risques du système financier, la Banque de France considère le risque cyber comme le risque structurel le plus élevé.

À cet égard, le règlement DORA constitue une avancée bienvenue en posant un cadre unifié d'exigences en matière de gestion des risques informatiques et cyber pour une très large gamme d'acteurs financiers – les banques, les assurances, les acteurs de paiement, les entreprises d'investissement, mais aussi les infrastructures des marchés ou les émetteurs de cryptoactifs. Tous ces acteurs doivent tester leur cyber-résilience et les plus systémiques d'entre eux seront assujettis à des tests d'intrusion pilotés par leur autorité de contrôle, afin de détecter d'éventuelles failles dans leur système d'information.

Le règlement DORA prévoit également un dispositif harmonisé pour les déclarations d'incidents cyber, informatiques et de paiement, afin que les autorités, dont l'Anssi, puissent orchestrer leurs réponses.

Enfin, ce règlement met en place une nouvelle surveillance des prestataires tiers critiques, dont la liste sera arrêtée au deuxième semestre de cette année par les autorités européennes de supervision. L'ACPR s'est préparée, au cours des deux dernières années, à assurer ces nouvelles missions.

Le règlement DORA est entré en application depuis le 17 janvier. La transposition de la directive va modifier plusieurs textes importants et le projet de loi Résilience introduit plusieurs dispositions qui nous semblent tout

à fait indispensables. Ainsi, en matière d'assujettissement, les sociétés de financement comme Crédit Logement ou l'Agence française de développement ne sont effectivement pas visées par le texte européen dans la mesure où elles ont un statut national. Mais si la loi n'inclut pas ces sociétés dans le dispositif, l'ACPR ne pourra pas juridiquement recevoir les notifications d'incidents ni contrôler les registres d'externalisation de ces acteurs importants pour l'économie française. C'est un point important, car le risque cyber est susceptible de se propager. Eu égard à l'interconnexion des acteurs du système financier, il est essentiel d'éviter d'avoir un maillon faible. La logique est donc bien d'unifier le traitement de l'ensemble des acteurs du système financier.

En outre, certains amendements au projet de loi nous sembleraient utiles. Il importe notamment d'étendre le périmètre de la directive aux succursales d'entreprises d'investissement de pays tiers. Concernant la charge administrative que cette directive sous-tend pour les entités supervisées, il nous semble utile de limiter la charge induite pour les infrastructures supervisées par plusieurs autorités, à savoir l'ACPR, l'AMF et la Banque de France. En effet, un guichet unique pour déclarer les incidents serait de nature à éviter une redondance des déclarations. Dans le même esprit, s'agissant des prestataires de services de paiement, il convient de simplifier le processus de déclarations d'incidents majeurs en les centralisant auprès d'une seule autorité, l'ACPR, en accord, bien sûr, avec la Banque de France.

M. Sébastien Raspillet, secrétaire général de l'Autorité des marchés financiers. – Merci de nous recevoir pour vous présenter la manière dont l'AMF s'est préparée à mettre en œuvre la directive DORA et vous parler concrètement des applications.

Dans une vie antérieure, j'ai négocié et finalisé, sous la présidence française du Conseil de l'Union européenne, le paquet Dora, la directive et le règlement. Il me revient aujourd'hui, au titre de l'AMF, de le mettre en application…

Le règlement DORA, la résilience opérationnelle numérique du secteur financier, s'inscrit dans un contexte de digitalisation croissante, comme l'a indiqué Frédéric Hervo, et d'externalisation importante. Les actions numériques ne sont pas toujours faites en interne. Aussi, les institutions financières doivent s'interroger sur les facteurs susceptibles de les conduire à interrompre un service.

L'AMF couvre un grand nombre d'entités, mais de taille plus petite que celles qui sont dans le champ d'activité de l'ACPR. Ce sont notamment les sociétés de gestion qui, au-delà du risque cyber, font appel à nous lorsqu'elles sont confrontées à un problème purement technique, telle une panne d'électricité, qui les prive de l'accès à leurs serveurs, et donc à leurs données. Outre les incidents cyber massifs, nous devons donc gérer quasiment au quotidien les incidents très pratiques que rencontrent ces sociétés de gestion de taille très variée.

Par ailleurs, avec l'entrée en vigueur quasi concomitante du règlement européen sur les marchés de crypto-actifs (Mica), les prestataires de services sur cryptoactifs vont passer d'une centaine d'acteurs à plusieurs dizaines.

Parmi les acteurs, nous comptons aussi les prestataires de services de financement participatif, ce que l'on appelait le *crowdfunding*.

Au-delà des autorités publiques qui se sont félicitées de l'adoption du paquet DORA, les investisseurs privés en Europe et outre-Atlantique reconnaissent que le règlement DORA a vocation à devenir un standard d'exigence minimale, qui suscite la confiance. Cette ambition est perçue de manière positive. De nombreux acteurs sont embarqués, car les domaines visés sont interconnectés. D'où l'intérêt de détecter les maillons faibles, comme l'a souligné Frédéric Hervo.

Il importe d'optimiser les ressources, car nous allons devoir faire face à des charges supplémentaires, comme la réalisation de tests de pénétration fondés sur la menace (TLPT, *Threat-Led Penetration Testing*), qui exige des compétences très pointues en termes de cyberexpertise, et la supervision des entités, une mission que nous exerçons déjà pour nous assurer du respect des réglementations européennes ou françaises, auxquelles s'ajouteront les réglementations fixées par le paquet DORA. En l'espèce, nous devrons être destinataires de la cartographie des prestations externalisées par les sociétés de gestion en vue d'identifier, le cas échéant, les éléments problématiques.

S'y ajoute notre mission de reporting. Parmi les entités critiques, nous n'avons que la plateforme de marché Euronext. Un point d'entrée unique entre les trois autorités de supervision serait effectivement une solution pertinente pour limiter la charge supplémentaire, il nous reviendrait alors d'assurer la transmission des informations, en lien avec l'Anssi. Il nous faut réfléchir à la procédure la plus efficace pour transmettre les données.

Nous subissons donc de manière indirecte les nouvelles charges imposées aux acteurs dans la mesure où notre mission de supervision sera accrue. D'où notre exigence d'efficience.

Pour illustrer mon propos, dans le domaine de la gestion d'actifs, par exemple, les petites et moyennes entreprises peuvent être victimes de *ransomware* ou d'intrusions prolongées dans les boîtes e-mail professionnelles, au même titre que les PME manufacturières. Le paquet DORA permettra à ces acteurs de mieux se protéger.

Pour ce qui concerne l'information des institutions financières, nous nous sommes efforcés de faire œuvre de pédagogie dans le cadre de nos actions classiques de supervision, en rendant nos acteurs attentifs à l'entrée en vigueur du règlement DORA. De nombreuses conférences, des webinaires et des séminaires ont été organisés à cette fin. Je pense que ces entités sont bien conscientes de l'importance de ces sujets, car les conséquences en termes d'image et de réputation sont très rapides.

Sans vouloir outrepasser mes prérogatives, d'après les témoignages que nous avons pu recueillir, l'Anssi est considérée par les institutions financières comme un tiers de confiance. Avec la directive NIS2, elle pourrait devenir une autorité de supervision, ce qui pourrait, de ce fait, modifier leur perception. Toutefois, il est à noter que nous avons un dialogue avec les entités que nous supervisons et n'hésitons pas à leur apporter des conseils en cas de besoin. Il pourra donc en être de même avec l'Anssi.

Le défi de l'AMF est d'être à la hauteur de ces nouveaux enjeux, avec le recrutement d'experts pour participer à l'amélioration de la prise de conscience des acteurs et à l'accroissement de la résilience, et ce au bénéfice de la santé globale du secteur financier en France et en Europe.

M. Frédéric Hervo. – Permettez-moi de revenir de manière plus détaillée sur certaines de vos questions.

Concernant l'articulation entre les directives DORA et NIS2, le considérant 16 et l'article 1er du règlement DORA en font une *lex specialis* de la directive NIS2. Pour le secteur financier, le règlement DORA a donc vocation à être le texte d'application, ce qui induit de fait une conformité des entités à NIS2.

Pour autant, l'Anssi reste pleinement partie prenante : cette autorité chargée de la cybersécurité répondra au premier chef sur le plan technique aux incidents cyber, ce qui implique une bonne coopération avec les autorités de contrôle du secteur financier.

Comme l'a indiqué Sébastien Raspiller, nous constatons une bonne connaissance des missions de l'Anssi par les acteurs du secteur financier. Depuis une vingtaine d'années, le groupe de place Robustesse, sous l'égide de la Banque de France, mobilise à la fois les grands acteurs du secteur financier, mais également les autorités publiques, telles que l'AMF, l'ACPR et l'Anssi, sur les risques opérationnels et les risques cyber, organise des tests et répond à des situations de crise. À cet égard, l'Anssi a participé à une table ronde sur la mise en œuvre du règlement DORA organisée, dans le cadre de la conférence de contrôle, par l'ACPR au mois de novembre dernier et à laquelle ont participé près d'un millier de participants.

Concernant les notifications d'incidents, nous sommes en capacité de les recevoir par le biais de différents acteurs en utilisant soit les circuits de notification habituels au reporting prudentiel, pendant les périodes ouvrées, soit la messagerie le dimanche ou en période de nuit. La temporalité et la criticité de ces notifications n'ont pas le même sens pour l'Anssi et les autorités de contrôle, qui ne jouent pas le même rôle en cas d'incidents cyber : l'Anssi apportera des réponses techniques et en informera les acteurs visés, tandis que les autorités de contrôle évalueront les conséquences de ces incidents pour le système financier et les différents acteurs concernés et aideront à ces derniers à prendre les mesures adéquates pour leurs produits financiers et leurs

services. Nos rôles sont complémentaires et ne sont pas substituables. Il est donc essentiel de maintenir une bonne coopération avec l'Anssi.

Vous avez évoqué la possibilité d'avoir une approche différente pour les sociétés de financement.

Permettez-moi de rappeler que ces établissements ont une activité de financement spécialisée, telle que l'affacturage, le crédit-bail, la caution ou l'octroi de garanties financières. Bien que ne collectant pas de fonds remboursables du public, leur activité est importante pour l'économie réelle. Les sociétés de financement présentent une certaine hétérogénéité en termes de taille et d'importance. Certaines entités sont critiques en raison de leur mission de service public, comme Action Logement ou l'Agence française de développement, ou de leur mission de cautionnement des prêts immobiliers résidentiels s'agissant de Crédit Logement, par exemple. En effet, cette société de financement a cautionné un encours de près de 430 milliards d'euros sur les 1 000 milliards d'encours de crédit immobilier en France. En cas de cyberattaque, la divulgation des données de millions de Français serait préoccupante. C'est la raison pour laquelle il importe d'appliquer le règlement à ces acteurs, même s'ils disposent d'un statut national. Je rappelle que près des deux tiers des sociétés de financement font partie de groupes bancaires. Il serait donc contre-intuitif que ces filiales ne soient pas soumises à cette réglementation, alors que les groupes bancaires le sont depuis le 17 janvier. Ce pourrait être là un maillon faible. Une mise en application du règlement DORA au début de l'année 2026 nous semble un délai raisonnable, sachant que nous appliquons toujours un principe de proportionnalité avec une approche par les risques dans nos activités de contrôle.

Pour ce qui concerne les textes réglementaires, deux normes techniques de réglementation sont encore attendues : l'une sur la sous-traitance et l'autre sur les TLPT, qui ont vocation à s'appliquer aux acteurs les plus systémiques. Ces tests commenceront vraisemblablement à la fin du premier semestre. Même si le règlement DORA est applicable depuis le 17 janvier, sa mise en œuvre est nécessairement progressive.

Mme Michelle Gréaume. – Concernant l'article 57 du projet de loi Résilience, qui introduit dans le code des assurances de nouvelles exigences pour les entreprises d'assurance et de réassurance pour renforcer la cybersécurité afin de protéger les données des assurés, comme les capacités de fonctionnement et d'indemnisation des assureurs. L'article 58 définit, quant à lui, les nouvelles obligations de gouvernance face aux risques liés à l'utilisation d'outils numériques. Comment comptez-vous renforcer la protection des contrats des assurés sur le plan numérique tant en ce qui concerne les données personnelles que financières ? Je pense aux assurances retraite, aux assurances vie ou encore aux assurances obsèques.

M. Frédéric Hervo. – Le règlement DORA aligne l'ensemble des acteurs quant à la gestion des risques informatiques, des risques

d'externalisation et des risques cyber. Il est effectivement important que le secteur de l'assurance soit bien protégé, au regard des données de santé, des données de paiement ou des données personnelles des assurés, qui sont toutes sensibles. Il appartiendra à l'ACPR de s'assurer, dans le cadre de ses missions habituelles de contrôle, que ce soit par un contrôle permanent sur une base documentaire ou sur place, que les établissements sont en conformité avec les normes réglementaires. Cela se fera dans le cadre d'une approche proportionnelle, par les risques, en fonction de la taille et du profil des acteurs, ainsi que de la nature de leur activité.

Mme Vanina Paoli-Gagin. – J'ai une question plus précise sur les fournisseurs de services *cloud*. Étant donné que ceux-ci ne seront pas nécessairement intra-européens, comment nous assurer de la sécurité des données qui seront hébergées ? Je pense notamment aux applications extraterritoriales des lois qui peuvent se multiplier au regard des changements géopolitiques qui ont lieu ces derniers temps.

Mme Hélène Conway-Mouret. – La France jouit d'une certaine indépendance en matière de défense, mais tel n'est pas le cas de nombre de nos partenaires européens. Un climat de confiance prévaut à ce jour, mais qu'en sera-t-il de notre souveraineté si la nature des relations venait à changer ? Sommes-nous en capacité d'héberger l'ensemble des données dont nous avons besoin, même si la construction d'un supercalculateur a été annoncée hier soir ?

Par ailleurs, ne risque-t-on pas de se retrouver avec des directives européennes qui vont tenir compte de l'ensemble des volontés des uns et des autres ?

M. Frédéric Hervo. – Ces deux questions nous permettent d'aborder l'un des piliers essentiels et très novateurs du règlement DORA, à savoir la mise en place d'un dispositif de surveillance des prestataires tiers critiques.

Les acteurs du secteur financier vont, au printemps, nous rapporter l'ensemble de leurs contrats d'externalisation avec les prestataires informatiques. Ces reportings passeront par les autorités compétentes, qui rétrocéderont ces informations aux trois autorités européennes de supervision, à savoir l'Autorité européenne des marchés financiers (Esma), l'Autorité bancaire européenne (ABE) et l'Autorité européenne des assurances et des pensions professionnelles (AEAPP). Sur la base de ces données, il sera possible d'identifier les prestataires qui, au regard de l'importance de leurs services, seront considérés comme critiques au niveau européen pour le secteur financier. On imagine aisément de quels acteurs il s'agit, notamment les prestataires de services de *cloud*, pour la plupart basés en dehors de l'Union européenne. Un dispositif de surveillance sera mis en place de manière conjointe par les autorités européennes de supervision pour vérifier si ces entités respectent le règlement DORA en termes de protection des données, de niveau de sécurité, de qualité des clauses contractuelles. D'ailleurs, ces

prestataires devront disposer d'une entité au sein de l'Union européenne, qui sera l'interlocutrice directe. Il s'agit donc là d'une innovation importante.

La liste de ces entités devrait être communiquée avant la fin de l'année 2025, avec une mise en œuvre effective du nouveau dispositif de surveillance au début de l'année 2026.

Enfin, les autorités nationales participeront à cet exercice de surveillance, à due concurrence de l'utilisation des services de ces prestataires par leurs acteurs financiers.

M. Akli Mellouli. – Vos explications sont source d'inquiétudes croissantes.

Je veux évoquer la question des collectivités territoriales, qui constituent un véritable enjeu. Quels mécanismes peuvent être mis en place pour les aider à financer leurs projets de cybersécurité ? Les assurances peuvent-elles jouer un rôle, notamment en matière de couverture, pour financer la cybersécurité de nos collectivités ?

M. Frédéric Hervo. – Votre première question concerne d'autres aspects du projet de loi Résilience qui ne relèvent pas de la compétence de l'ACPR.

Concernant votre seconde question, nous constatons le développement d'un certain nombre de contrats spécifiques pour assurer le risque cyber. Les contrats d'assurance comportent une tarification associée au niveau de risque.

M. Sébastien Raspiller. – Je vous l'ai dit, j'ai négocié le paquet DORA lors de la présidence française du Conseil de l'Union européenne. Nous avions alors beaucoup insisté sur la nécessité d'avoir une capacité d'action en termes de supervision en Europe. Certes, je ne réponds pas là à votre interrogation concernant notre souveraineté, mais nous avons obtenu l'obligation d'avoir une entité implantée dans l'Union européenne.

La liste des entités tiers critiques sera arrêtée à la fin du premier semestre. En France, les autorités de régulation financière sont soumises par l'Anssi au *SecNumCloud*. Certes, cette obligation a un coût, mais elle est de nature à apporter une sécurité. En revanche, nos homologues ne sont pas réceptifs à la mise en place d'un *cloud* européen, alors que nous traitons de données confidentielles très sensibles. C'est pourquoi il importe collectivement de faire un minimum de pédagogie afin de contribuer à une prise de conscience des risques auxquels nous pouvons collectivement faire face, et le paquet DORA y participe.

Une cyberattaque sur une petite structure peut avoir des effets dévastateurs. La connaissance des sous-traitants permet d'en diminuer la probabilité. Il faut organiser des campagnes de *phishing* et de sensibilisation aux risques pour améliorer la résilience. Les structures que nous supervisons, y compris de plus petite taille, sont sensibilisées à ces questions. Cela ne

signifie pas que tout risque est éliminé – toute entité, y compris locale, connaît une cyberattaque –, mais cela diminue sans aucun doute la probabilité de les subir. C'est pourquoi DORA impose des exigences de reporting rapide et structuré des incidents pour éviter de graves impacts. Le secteur financier a été sensibilisé à cette question bien avant la mise en place du règlement DORA. Cependant, celui-ci a pour effet de structurer, de professionnaliser et de systématiser la résilience, y compris dans d'autres secteurs.

Mme Catherine Morin-Desailly. – Vos explications ne sont pas de nature à nous rassurer. Les données les plus sensibles de nos administrations, des Français et des Européens d'ailleurs sont confiées aux trois principaux fournisseurs de services *cloud* que sont AWS, Google et Microsoft, qui dominent très largement le marché.

Je m'inquiète moins du *Cloud Act* que de la section 102 du *Foreign Intelligence Surveillance Ac*t (Fisa), renouvelée pour deux ans par Ursula von der Leyen et Joe Biden au lendemain de l'annulation, le 16 juillet 2020, du cadre de transfert de données entre l'Union européenne et les États-Unis, le *Data Privacy Shield*. Le Fisa permet le transfert des données des Européens sur simple requête de l'État fédéral. Un Européen peut donc se voir transférer ses données sans avoir reçu de notification, contrairement à un Américain. D'où notre crainte d'un nouveau renouvellement avec l'arrivée de Donald Trump.

M. Frédéric Hervo. – Le règlement DORA vise à répondre au risque d'attaques cyber, mais n'a pas vocation à répondre à l'ensemble des problématiques associées à l'utilisation des services en nuage, tels que les risques de corruption, de divulgation des données liées à des attaques malveillantes ni aux questions de coopération internationale ou de droits en la matière applicables par différents États. Le règlement DORA s'attache à la prévention du risque cyber d'une manière plus générale.

M. Olivier Cadic, président. – Même si trois acteurs occupent 70 % du cloud, n'oublions pas OVHcloud, un acteur français, qui est un leader européen.

Permettez-moi d'aborder un sujet d'actualité, l'intelligence artificielle (IA). J'ai demandé à un outil d'IA s'il pouvait me donner des conseils financiers. Il a orienté ma question en me demandant quels types de conseils je souhaitais obtenir – gestion du budget, investissement, épargne, immobilier, retraite, etc. Ces conseils sont donc parfaitement possibles aujourd'hui.

Un nouvel acteur, apparu il y a deux semaines, a eu un impact majeur sur les cours de bourse. Va-t-il être régulé, contrôlé par vos services ?

M. Sébastien Raspiller. – Nous avions fait ce test il y a quelque temps et l'outil nous avait répondu qu'il n'était pas autorisé, d'après la réglementation, à nous donner des conseils financiers, mais qu'il pouvait quand même le faire…

C'est une question que nous examinons au sein de l'Organisation internationale des commissions de valeurs (IOSCO, *International Organization of Securities Commissions*), qui regroupe quelque 130 pays. Cette organisation permet à nos enquêteurs de demander des informations sensibles à nos homologues.

Nous avons engagé une réflexion à ce sujet, mais je ne puis vous répondre, car la territorialisation est une question complexe.

Dans un contexte de digitalisation croissante des activités de l'économie, voire du quotidien, la mission première que nous a confiée le législateur ne concerne plus que la vérification du conseil bancaire. Il nous faut développer des outils de veille des réseaux sociaux. Nous avons, par exemple, développé, en coordination avec l'Autorité de régulation professionnelle de la publicité (ARPP), un certificat de l'influence responsable pour les influenceurs. L'intelligence artificielle va bouleverser les choses ; il nous faut sans cesse remettre l'ouvrage sur le métier. Nous nous efforçons de contribuer, à notre échelle, au sein de ce forum mondial à définir des lignes directrices susceptibles d'apporter des réponses satisfaisantes en matière de protection de l'épargne.

M. Olivier Cadic, président. – Je vous remercie de votre participation.

2. Les entreprises de cyberdéfense – Audition d'Airbus, Orange et Thales

M. Olivier Cadic, président. – Nous poursuivons notre cycle d'auditions publiques par une table ronde réunissant des groupes du secteur de la cyberdéfense.

Le groupe Airbus est représenté par M. Michaël Barthellemy, *Heaf of Cyber Risk and Assets Management* du groupe Airbus, et par M. Olivier Masseret, directeur des relations institutionnelles.

Le groupe Orange est représenté, pour sa propre sécurité, par M. Patrick Guyonneau, directeur de la sécurité du groupe Orange, et, pour la fourniture de services de cyberdéfense, par M. Olivier Bonnet de Paillerets, général, ancien directeur adjoint de la direction générale de la sécurité extérieure (DGSE) et maintenant *Executive Vice President Technology & Marketing* de la filiale Orange Cyberdefense. Ils sont accompagnés de M. Laurentino Lavezzi, directeur des affaires publiques.

Enfin, le groupe Thales est représenté par M. Alexis Caurette, vice-président stratégie cybersécurité, et par Mme Isabelle Caputo, directrice des relations institutionnelles.

Je vous remercie d'avoir accepté de venir nous livrer votre vision globale du projet de loi qui vise à transposer trois directives : la directive sur

la résilience des entités critiques, dite REC, dans le titre Ier ; la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite NIS 2, dans le titre II ; et la directive sur la résilience opérationnelle numérique du secteur financier, dite DORA, dans le titre III.

Vous êtes tous, à votre niveau, directement concernés par ce projet de loi, comme vous l'étiez d'ailleurs par la directive NIS 1, en tant qu'acteurs majeurs du secteur de la défense et du secteur civil.

Vos groupes se caractérisent également par une dimension européenne et internationale. Votre regard sur le marché européen et les risques de distorsion juridique de transposition dans les différents États membres de l'Union européenne nous sera donc très utile.

Enfin, outre le souci de votre propre sécurité, vous fournissez des services de cybersécurité à vos clients, entreprises ou collectivités territoriales, par le biais de vos filiales – Airbus Protect, Orange Cyberdefense ou Thales Solutions de cyberdéfense. Là aussi, nous serons à l'écoute de vos points de vue sur l'impact du projet de loi.

Avant de vous céder la parole, je rappelle à tous que cette audition fait l'objet d'une captation vidéo qui est retransmise sur le site internet du Sénat puis consultable en vidéo à la demande.

M. Patrick Chaize, rapporteur. – En ma qualité de rapporteur chargé de l'examen du titre II de ce projet de loi, mon intervention sera centrée sur la transposition de la directive NIS 2.

Cette directive est d'une importance capitale : les changements qu'elle implique pour le monde économique sont significatifs dans toute l'Union européenne, mais plus particulièrement en France.

D'abord, le nombre d'entités régulées passe de 500 à 15 000 et le nombre de secteurs économiques de 6 à 18 par rapport au précédent cadre de régulation fixé par la directive NIS 1.

Ensuite, ce sont désormais tous les systèmes d'information des entités régulées qui sont, par principe, concernés.

Enfin, c'est un changement majeur de paradigme qui est à l'œuvre : il ne s'agit plus seulement de sécuriser des infrastructures critiques, mais aussi d'assurer la résilience des entités critiques en tant qu'organisations. Autrement dit, la couverture est beaucoup plus large.

Je me réjouis donc aujourd'hui d'entendre l'analyse des experts de la cyberdéfense que vous êtes sur le projet de loi de transposition de la directive NIS 2.

Pouvez-vous tout d'abord nous indiquer quelles solutions de cyberdéfense vous développez, et à l'attention de quels clients ? La directive NIS 2 aura-t-elle un impact très important sur vos activités ?

Quelle analyse faites-vous ensuite du projet de loi ? Considérez-vous qu'il assure une transposition fidèle de la directive ? Identifiez-vous un risque de surtransposition ou, *a contrario*, de sous-transposition ?

Sur la procédure de notification des incidents, alors que la directive NIS 2 prévoit la transmission, « sans retard injustifié », d'une alerte précoce dans un délai de vingt-quatre heures puis la transmission d'une notification d'incident dans un délai de soixante-douze heures, le projet de loi ne mentionne pas ce double délai, contraignant les entités à notifier leurs incidents « sans délai » et évoquant la notification « d'incidents critiques » plutôt que « d'incidents importants ».

Que pensez-vous de ces choix ? Sont-ils de nature à surtransposer ou à sous-transposer la directive et, surtout, sont-ils de nature à affaiblir ou à renforcer notre réponse collective aux cybermenaces ?

S'agissant du périmètre, le Gouvernement a opéré trois choix qui soulèvent des interrogations : l'inclusion des établissements d'enseignement menant des activités de recherche ; l'inclusion des collectivités territoriales, notamment les départements, les métropoles, les communautés urbaines, les communautés d'agglomérations et les communes de plus de 30 000 habitants ; enfin, l'élargissement du périmètre des entreprises concernées, puisque les critères de taille et de chiffre d'affaires sont fixés alternativement tandis que les textes européens les fixent cumulativement. Que pensez-vous de ces choix ?

Enfin, les entreprises et les collectivités territoriales vous semblent-elles suffisamment informées des changements à venir ?

M. Michaël Barthellemy, *Head of Cyber Risk and Assets Management* du groupe Airbus. – Enjeu crucial pour les organisations, notamment pour les organisations critiques désormais catégorisées en « entreprises essentielles » et « entreprises importantes », la résilience digitale peut se définir comme la capacité à anticiper, prévenir, dissuader, détecter, et retarder les attaques, y répondre, résister et se remettre des incidents de cybersécurité.

Le but est de protéger l'intégrité informatique et fonctionnelle, de limiter les pertes financières ainsi que la dégradation de l'image et de la confiance, d'assurer la continuité des activités et le maintien de la productivité malgré les attaques, y compris en mode dégradé, de préserver et de sécuriser les données, en particulier dans le contexte du règlement général sur la protection des données (RGPD).

Cette résilience, lorsqu'elle parvient à être démontrée, conditionne l'instauration d'un climat de confiance avec nos clients, nos usagers, nos fournisseurs et nos autorités de tutelle.

Nos organisations doivent également de plus en plus s'assurer contre le préjudice que représenterait une disruption majeure et démontrer aux assureurs et cyberassureurs leur potentiel de résilience.

Je souhaiterais à présent attirer votre attention sur quelques points qui ressortent de notre étude du projet de loi.

Sans vouloir déposséder le Parlement français de ses prérogatives, il ne nous semble plus envisageable aujourd'hui que ce type de mesures soient véhiculées par une directive. Elles devraient impérativement faire l'objet d'un règlement européen. Imaginez en effet la difficulté pour un groupe comme Airbus, présent dans la quasi-totalité des États membres de l'Union, de devoir appliquer vingt-sept réglementations différentes…

Il faut ensuite analyser plus globalement l'impact de la réglementation sur la compétitivité des entreprises européennes dorénavant régulées. Le projet de loi, dans la continuité des dispositifs existants, apparaît pour notre filière comme une double surtransposition de la directive européenne. La France dépasse les demandes de la directive et la proposition de transposition actuelle vient doublonner un certain nombre de contraintes déjà présentes dans le corpus réglementaire en vigueur – loi de programmation militaire, instruction générale interministérielle n° 1300, instructions interministérielles n^{os} 900 et 901.

L'augmentation des sanctions fera également peser une pression financière sur nos entreprises. Nos concurrents internationaux, y compris européens, qui ne sont pas soumis à ces règles, seront avantagés. Veillons à ne pas créer par surtransposition une opportunité de dumping de cybersécurité pour les autres États membres.

Nous nous soucions également de l'articulation de ces nouvelles dispositions avec les autres réglementations existantes, nationales et européennes, et nous demandons à ce que le délai pour satisfaire à ces différentes transpositions soit étendu.

Les PME et les entreprises de taille intermédiaire (ETI), déjà vulnérables, pourraient être les premières fragilisées par des exigences trop contraignantes et une mise en œuvre précipitée. Nous devons leur laisser le temps nécessaire de se conformer aux nouvelles règles.

Les questions de souveraineté numérique et d'indépendance géostratégique nous préoccupent aussi. La résilience opérationnelle vient parfois contredire le principe de souveraineté, notamment dans les domaines où les Gafam – Google, Apple, Facebook, Amazon, Microsoft – prennent une place prépondérante. Les choix qui seront faits aujourd'hui détermineront notre capacité à maintenir demain l'équilibre entre indépendance et interdépendance, dans un contexte de concurrence globale.

Enfin, pour que nos entreprises puissent réussir cette transition vers NIS 2, un soutien des services de l'État, au bon niveau, sera indispensable :

soutien technique et financier, aide au développement de solutions de confiance adaptées aux PME et aux ETI, etc. Nous pensons que l'Agence nationale de la sécurité des systèmes d'information (Anssi) doit jouer un rôle prépondérant dans ce dispositif.

M. Laurentino Lavezzi, directeur des affaires publiques du groupe Orange. – Nous sommes concernés à double titre par ce projet de loi : en tant qu'entreprise essentielle, nous devrons nous soumettre aux nouvelles obligations ; en tant que fournisseur de services, nous pourrons voir quelques marchés s'ouvrir à nous.

Nous partageons les préoccupations de Michaël Barthellemy sur la cohérence et l'articulation des différentes réglementations. Il sera d'autant plus facile d'appliquer ces nouvelles obligations qu'elles seront peu ou prou les mêmes partout en Europe.

Nous nous soucions aussi de la compétitivité de nos entreprises et d'un risque de surtransposition, y compris au niveau des règlements d'application. Nous souhaitons donc que le Parlement encadre autant que possible le champ d'intervention du pouvoir réglementaire.

L'application de la loi de l'établissement principal pourrait en effet conduire, en cas de surtransposition en France, à des asymétries entre acteurs d'un même marché.

M. Patrick Guyonneau, directeur de la sécurité du groupe Orange. – Il n'est pas toujours aisé d'appréhender dans le détail les obligations qui s'imposent à nous. Ainsi, pour notre activité d'opérateur de télécommunications, nous sommes soumis à la fois à NIS 2 et aux dispositions concernant les opérateurs d'importance vitale (OIV). En revanche, pour nos activités numériques, nous sommes concernés par l'ensemble des mesures du projet de loi. Il arrive pourtant fréquemment qu'un même système d'information ait plusieurs finalités.

Par ailleurs, comme l'a souligné Laurentino Lavezzi, dès lors que le droit du siège prévaut, toute transposition maximaliste de la directive risque de nous handicaper, car nous sommes présents en Slovaquie, en Pologne, en Belgique, au Luxembourg, en Espagne et en Moldavie, des pays où les droits locaux sont moins restrictifs qu'en France. Les directives adressées par Orange à ses filiales pourraient donc être plus contraignantes que les règles locales.

Était-il opportun d'inclure les collectivités locales dans le champ du texte ? À notre sens, oui, en raison notamment d'une spécificité française, les réseaux d'initiative publique (RIP) en matière de télécommunications. En excluant les collectivités locales, on risquait sans doute d'exclure les RIP et de créer des points de faiblesse. Or il est très important d'assurer une continuité dans les communications, en particulier pour les appels d'urgence.

M. Olivier Bonnet de Paillerets, ***Executive Vice President Technology & Marketing*** **d'Orange Cyberdefense**. – Orange Cyberdefense est

une société anonyme de services et de sécurité numériques détenue par le groupe Orange qui couvre l'ensemble du champ du marché de la cybersécurité : détection et analyse de la menace, protection et gestion de crise.

Le marché de la cybersécurité reste très dynamique, en croissance de 11 % à 12 % par an jusqu'en 2030 selon les analystes. C'est un marché très fragmenté et très concurrentiel. Nous sommes leader en Europe avec 12 % de parts de marché, 5 % en Belgique.

Nous faisons face à des niveaux de complexité de plus en plus élevés. En Europe, le deuxième continent le plus visé après les États-Unis, la cybercriminalité continue de croître de 20 %, et même de 57 % cette année si l'on considère les petites et moyennes entreprises.

Les nouvelles menaces, en provenance des activistes, ont un impact croissant sur les sociétés, avec des actions de désinformation couplées à des actions de saturation de type DDoS (attaque par déni de service distribué).

La régulation qui s'impose aux entreprises devient elle-même de plus en plus complexe.

Enfin, le mouvement vers le *cloud* accroît la « surface d'attaque » des entreprises.

Pour nos clients, tout cela devient trop compliqué, ils ont besoin d'être accompagnés.

En tant que société numérique, nous sommes également visés par le règlement d'exécution de l'Union européenne d'octobre 2024 comme entreprise essentielle. Cela représente un coût pour nous, certes marginal, car nous avions déjà toutes nos certifications Anssi, mais surtout un changement culturel important. Nous devrons en effet garantir que tout nouveau service de sécurité que nous lançons soit conforme à NIS 2, ce qui nécessite un investissement important. Mais cette évolution nous semble positive, car elle consolide notre réputation.

C'est aussi une opportunité pour nous. Avec NIS 2, de plus en plus d'entreprises seront concernées par cette double complexité et nous devons investir ce marché très rapidement, en accompagnant ces entreprises par de nouveaux services.

Sur la transposition elle-même, je suis moins préoccupé que mes collègues, car j'y vois pour nous de nouvelles opportunités. Mais le diable peut se cacher dans le détail des décrets d'application, et il reste des questions sur les processus de remontée d'incidents, les certifications et les qualifications. N'est-ce pas l'occasion de les simplifier et d'avoir des parallèles de conformité ? L'Anssi aura un rôle majeur à jouer dans la rédaction de ces décrets.

M. Alexis Caurette, vice-président stratégie cybersécurité du groupe Thales. –Je suis chargé de la stratégie des activités de services en cybersécurité et des offres associées au niveau du groupe.

Nous sommes à la fois éditeur de logiciels et constructeur de solutions de cybersécurité pour protéger ces derniers. Nous accompagnons aussi plus globalement nos clients dans la gestion de leur risque cyber en développant des services de *security operations center*, c'est-à-dire des services de détection et de réponse aux attaques, partout en Europe.

Nous nous concentrons plus spécialement sur l'accompagnement des grands groupes et des opérateurs d'importance vitale du secteur bancaire.

Comme vous l'avez rappelé, monsieur le rapporteur, le nombre d'entités régulées va passer de 500 à 15 000 avec la directive NIS 2. La cybersécurité va dépasser le cadre des systèmes d'information sensibles pour évoluer vers une notion de résilience à grande échelle. La marche à gravir sera importante, et il nous semble fondamental d'accompagner le déploiement de ces normes européennes par une politique industrielle claire de cybersécurité axée sur le développement d'offres capacitaires suffisantes pour permettre aux entités essentielles et importantes de se mettre en conformité avec NIS 2 et de rehausser leur niveau de maturité et de résilience cyber.

Face à cette forte croissance du périmètre couvert, avec des acteurs qui n'auront pas forcément toutes les capacités pour monter en compétences, le risque est réel de voir émerger des offres *low cost*, qui permettront de cocher la case « conformité », mais sans réalité opérationnelle derrière.

La mise en œuvre de la loi de programmation militaire a contribué au développement d'une politique industrielle autour des schémas de qualification de services. Ces schémas ont permis d'accroître le niveau d'exigence, non seulement vis-à-vis des OIV, mais surtout vis-à-vis des offreurs. Il est important de prendre cela en compte, et de réfléchir à la mise en place d'une politique industrielle qui permette la construction d'une offre répondant aux besoins. Ce ne sera certes pas l'offre qui a été développée avec la loi de programmation militaire – le cadre est probablement trop contraignant, les enjeux liés à la sécurité tenant plus de la souveraineté que de la résilience –, mais il faut une politique qui garantisse une offre de qualité, tout en permettant agilité et compétitivité.

Il nous semble donc fondamental d'associer, à la fois, les nouveaux régulés et les acteurs de l'offre dans la réflexion sur cette politique industrielle, sur les nouveaux labels ou schémas de certification qui permettraient d'encourager la mise sur le marché d'offres de bonne qualité, dans un contexte où l'on s'attend à une accélération très forte de la demande.

Cette politique industrielle pourrait être associée à un soutien au financement ou développement d'offres spécifiques, de cadres – ou *frameworks* – de mise en conformité. Le déploiement de solutions autour de l'intelligence artificielle (IA) pour la cybersécurité permettrait également d'accompagner la mise à l'échelle. Enfin, se posent des questions de formation des donneurs d'ordre et des opérateurs.

Je veux par ailleurs revenir sur le sujet des remontées d'incidents qui a été mentionné, avec des exigences en termes de délais et de niveau de sécurité. Sur ce volet, il s'agit bien, avec la transposition de la directive, d'améliorer la vision qu'ont les États et la Commission européenne de l'état de la menace, pour anticiper d'éventuelles crises cyber majeures. Il me semble néanmoins que la boucle descendante n'est pas suffisamment modélisée et mise en avant : faire remonter l'information, c'est bien, mais ce sont les acteurs exposés au risque et à la menace qui en ont besoin ; or il y a peu de clarification sur la façon dont l'information redescend.

Nous considérons le traitement de cet aspect relativement faible dans les textes. Le partage d'information devrait être renforcé, avec le développement d'une offre de renseignement d'intérêt cyber – ou *Cyber Threat Intelligence* dans le jargon américain – qui serait mise à la disposition des entités essentielles et importantes, mais que celles-ci pourraient également actionner. Aujourd'hui, un certain nombre d'informations, qui concernent notamment le contexte de la menace – écosystème des acteurs malveillants, modes opératoires, etc. –, circulent peu, alors qu'elles sont fondamentales pour améliorer la résistance et la résilience des entités intermédiaires.

S'agissant du risque de surtransposition, notons qu'il y aussi de la sous-transposition à certains endroits du texte. L'enjeu pour nous, c'est celui de la compétitivité : il ne faut pas qu'une surtransposition vienne compromettre l'accès des entités régulées aux marchés européens. L'hétérogénéité entre réglementations nationales que créent les surtranspositions ou sous-transpositions nous posent également des problèmes, car en tant qu'acteur de la cybersécurité français à vocation européenne, nous cherchons à exploiter les offres que nous avons développées sur l'ensemble du territoire européen.

Enfin, sur le périmètre et l'inclusion des collectivités territoriales, je donnerai plutôt un avis personnel : les enjeux en termes d'expositions cyber sont tels pour ces organisations, avec des risques économiques, mais aussi des risques sur l'image du service public, qu'il me paraît indispensable de les accompagner dans leur montée en maturité.

M. Patrick Chaize, rapporteur. – Ce que je souhaite précisément savoir, c'est si des points essentiels du texte du Gouvernement vous paraissent déjà relever de la surtransposition ou de la sous-transposition. Je ne vous demande pas de me les citer maintenant, mais il serait très intéressant pour nous d'avoir une réponse écrite de votre part sur ce sujet.

M. Patrick Guyonneau. – Les sujets clés sont la définition des incidents – nous sommes un peu dans le flou sur ce point – et les délais pour signaler ces incidents. Nous sommes trois groupes mondiaux autour de la table : est-ce, par exemple, le siège qui doit déclarer ? À ce stade, il est écrit qu'il faut remonter n'importe quel incident dans une filiale européenne à Paris, en vue d'une déclaration à l'Anssi. Cela a-t-il vraiment du sens ?

M. Olivier Cadic, président. – Et c'est sans parler du retour de l'information… C'est pourquoi, comme l'a indiqué Patrick Chaize, nous souhaitons connaître vos frustrations ou les limites que vous constatez. Vos propos rejoignent complètement certains commentaires entendus lors d'auditions d'experts de l'écosystème, et vous venez en réalité conforter une préoccupation que nous avons depuis le début. Notre objectif est bien que ce texte serve à aider les entités à mieux se défendre, non à leur compliquer la vie.

Avant de passer la parole à mes collègues, je veux porter à votre connaissance les questions de l'un de nos rapporteurs, Hugues Saury.

Celui-ci souhaite tout d'abord savoir si le choix du Gouvernement de confier à une autorité unique, sauf exception pour la défense, la mise en œuvre de la politique gouvernementale en matière de sécurité des systèmes d'information vous paraît pertinent.

Il s'interroge également sur le regard que vous portez aux définitions inscrites à l'article 1er du projet de loi : activité d'importance vitale ; infrastructure critique ; point d'importance vitale et système d'information d'importance vitale. Au cours de précédentes auditions, plusieurs personnes ont regretté l'absence de définition des notions d'incident et de vulnérabilité, notamment d'origine humaine. Hugues Saury souhaitait vous interroger sur ce point précis, mais je crois que le constat est unanime…

Mme Audrey Linkenheld. – Ma question, certes un peu décalée, me permet néanmoins de rebondir sur certains propos concernant la sécurisation du *cloud*. Nous le savons, la plupart des grands acteurs de ce domaine ne sont pas européens, mais c'est aussi vrai pour les prestataires. C'est un des points d'alerte que nous avions identifiés, avec ma collègue Catherine Morin-Desailly, lors d'un travail sur une proposition de résolution européenne relative à la cyber réserve. J'ai conscience que le projet de loi traite plutôt de la prévention en amont, mais, considérant qu'une cybermenace peut se transformer en cyberattaque, peut-on profiter de votre présence pour évoquer l'aval ? Pouvez-vous nous éclairer sur la question des prestataires en cas d'intervention à mener ? Des éléments viennent-ils vous conforter ou vous fragiliser dans le texte que nous examinons ?

M. Michaël Barthellemy. – Je peux vous confirmer l'existence de la cyber réserve, puisque j'en fais partie à titre personnel. Cela étant dit, nous avons déjà monté des groupes d'entraide au sein de la filière, ces groupes ayant vocation à aider un acteur qui en aurait besoin. Cette avancée a été permise par la mise en œuvre de la loi de programmation militaire, dont le but était tout de même d'accroître le niveau global de résilience cyber. Le projet de loi, dans sa rédaction actuelle, semble aller en sens inverse, en formulant une demande assez forte de démonstration de preuve. Cela peut être contre-productif sur le plan de l'efficacité économique. En effet, tout l'argent que les

entreprises mettront à démontrer qu'elles sont conformes, elles ne l'emploieront pas autrement.

Cela rejoint la question de l'Anssi. Oui, nous souhaitons que l'Agence soit le point, non unique, mais central. Depuis que celle-ci est montée en compétences, tout fonctionne beaucoup mieux.

L'écosystème doit être bipartite : l'État, d'un côté, et les différents intervenants privés ou publics, de l'autre. Tous doivent se mettre d'accord sur les preuves attendues et les groupes d'intervention auxquels on pourra faire appel en cas de sinistre. Pour donner un exemple, Airbus a réfléchi à la façon dont on pouvait, au niveau de l'assurance cyber, travailler en filière : de la sorte, un risque systémique qui surviendrait sur la filière bancaire serait moins susceptible d'affecter la filière industrielle, laquelle pourrait alors venir en aide à la première.

M. Olivier Bonnet de Paillerets. – Si j'ai bien compris, madame la sénatrice, vous évoquez la réserve de l'Union européenne. Celle-ci soulève un dilemme : peut-on accepter que des sociétés de services non européennes en fassent partie ? La bonne équation, selon moi, est de faire en sorte que les entreprises de l'Union européenne soient *primus inter pares* dans l'intervention, avec la possibilité d'être accompagnées par des sous-traitants non européens.

S'agissant de l'Anssi, la maturité face au numérique progresse moins vite que le numérique lui-même, qui s'impose dans les organisations. C'est pourquoi, pour ma part, je préfère que l'on sous-transpose, à condition que l'on renforce dans le même temps le rôle de l'Anssi.

M. Alexis Caurette. – Nous sommes en train de parler de sécurité et de résilience d'organisations qui n'ont pas forcément un enjeu en termes de souveraineté. La question est de savoir si, pour ces organisations, il est possible de sécuriser correctement des charges déployées dans des *clouds* qui peuvent être parfois globaux. Je le pense, mais cela doit s'accompagner des bonnes solutions et du bon niveau de maturité. La transposition de la directive NIS2 sous-tend une approche par le risque : il n'y a pas de raison de penser que nous serions incapables de mener des analyses de risques au niveau de l'entité, indépendamment de l'origine du *cloud*, et de déployer les bonnes mesures de protection.

Sur la cyber réserve européenne, il y a un enjeu autour du maintien de capacités locales dans chaque pays. En effet, les capacités régaliennes sont considérées comme étant d'abord au service de la résilience de l'État ; quant à la participation à une résilience européenne, elle incombera aux entreprises privées… Malheureusement, nous sommes actuellement en sous-capacité de réponse à un incident cyber en Europe. On ne peut donc pas faire l'économie de se tourner vers quelques acteurs pertinents. Mais je suis tout à fait d'accord avec Olivier Bonnet de Paillerets, il faut que la coordination ne relève que

d'entreprises européennes car nous ne savons pas dire, aujourd'hui, d'où viendront les attaques.

La question de la surtransposition ou de la sous-transposition dépendra aussi des décrets d'application qui, j'imagine, seront sectoriels. C'est là toute la complexité du sujet. Nous sommes à la croisée des chemins entre l'expertise cyber et l'expertise de chaque secteur. Qu'une entité unique soit garante du respect du processus de transposition et de son homogénéité est une bonne chose, mais il faudra s'assurer que l'Anssi, par le biais de collaborations ou de ressources propres, dispose de l'expertise sectorielle nécessaire pour pouvoir prendre en compte les enjeux spécifiques des différents marchés.

Mme Michelle Gréaume. – Comment les entreprises de cyberdéfense comptent-elles collaborer avec le nouveau régiment de cyberdéfense de l'armée de terre et quelles actions sont mises en œuvre pour assurer la défense des intérêts français ?

Par ailleurs, quels efforts de formation pourraient être engagés par vos entreprises ? Dans le domaine de la cyberdéfense, quel objectif de formation comptent-elles atteindre ?

Mme Vanina Paoli-Gagin. – On sent bien qu'une approche systémique est nécessaire, dès lors que notre objectif est la robustesse du dispositif dans son ensemble. Envisagez-vous la possibilité d'une coconstruction public-privé des cahiers des charges qui prédéterminent les offres, ou d'une mise à disposition de « patrons » ? Les collectivités locales ne disposent pas nécessairement d'acheteurs publics capables de concevoir de telles offres.

M. Michaël Barthellemy. – La collaboration avec « l'arme cyber » se fait non pas de manière directe, mais au travers de l'Anssi. Nous communiquons des analyses de menaces et examinons les indicateurs de compromission que nous avons pu trouver.

En ce qui concerne la formation, on constate que de plus en plus de cursus sont mis en place. Nous aurons, demain, des wagons de professionnels, mais il faudra réussir à les garder chez nous, car – il ne faut pas se voiler la face – ceux qui sont extrêmement bons partent à l'étranger…

En ce qui concerne les offres groupées, l'analyse des différentes réglementations au niveau européen montre que nous devons gérer 3 500 contraintes… Si nous pouvions avoir demain une offre « tamponnée » par l'Anssi – elle validerait qu'une solution répond à une majorité des contraintes prévues dans les différentes lois –, nous ferions un grand pas en avant !

M. Olivier Bonnet de Paillerets. – Le monde de l'entreprise et celui de l'État ne se connaissent pas encore suffisamment, en particulier dans le domaine numérique, alors qu'ils sont confrontés à des enjeux communs en

matière de souveraineté et d'innovation. Il nous faut recréer, imaginer ou développer d'autres formes de partenariats.

J'étais déjà très favorable aux partenariats lorsque j'étais commandant de la cyberdéfense au ministère des armées, je le suis encore plus maintenant que je travaille dans le monde de l'entreprise. Nous avons, par exemple, créé un cadre d'échanges entre des officiers qui viennent pendant trois ans au sein d'Orange Cyberdefense et des ingénieurs d'Orange qui partent travailler dans les armées, afin que chacun s'imprègne de la culture de l'autre. Ces petits pas me semblent essentiels pour la connaissance mutuelle.

Nous portons une attention particulière aux collectivités locales parce que la descente dans le bas de marché et au niveau territorial de l'offre cyber est de plus en plus critique. On se doit de proposer aujourd'hui des services « sur étagère », très faciles d'accès, qu'on appelle « *plug and play* », permettant à des non-initiés de disposer immédiatement de services cyber. Cela nécessite que nous nous rapprochions davantage des collectivités.

M. Patrick Guyonneau. – Le groupe Orange compte 250 à 300 réservistes ; nous avons des conventions avec les armées pour organiser leur disponibilité. Pendant les jeux Olympiques, nous avons mis à la disposition des forces de la gendarmerie un certain nombre de spécialistes cyber. Ce dispositif est intéressant, car il permet un échange de cultures, et des échanges opérationnels en fonction des besoins.

Dans l'une des versions du projet de loi, un article portait sur les opérateurs soumis à l'application du code des marchés publics. Il serait intéressant que cet article permette de promouvoir les services proposés par des entreprises nationales. Quand il s'agit d'analyses de risques d'une université qui fait de la recherche, je ne comprends pas que l'on fasse un marché ouvert ! Des critères extrafinanciers peuvent également être mis en place : par exemple, le prestataire accueille-t-il des réservistes ? Car mettre un certain nombre de spécialistes à disposition au travers de la réserve fait partie de notre contribution à l'œuvre commune de défense.

Nous avions fait, dans le cadre de la filière des industries de sécurité, des offres d'expertise et de renforts de sécurité qui avaient très bien fonctionné pour les hôpitaux, en 2021-2022 dans le cadre de France 2030. Nous attendons la relance de cette filière, avec des offres non seulement pour les systèmes de santé, qui sont fortement soumis à des cyberattaques, mais aussi pour les collectivités locales.

M. Olivier Bonnet de Paillerets. – Nous sommes en train de modifier nos formations pour sortir du mode « les experts parlent aux experts » et former les cadres dirigeants, les « *C-Level* », à la question cyber et à la gestion de crise, notamment dans les comités exécutifs (comex). Nous pouvons encore faire des gains de maturité extrêmement importants, qui permettent depuis le haut de faire descendre et d'infuser une compréhension des contraintes et des enjeux de cybersécurité.

M. Alexis Caurette. – Les grands groupes tels que les nôtres ont pratiquement tous développé des filières internes de formation à la cyber. J'ai observé cette tendance, à la fois, dans de grands groupes offrant des solutions cyber, mais également dans le domaine bancaire, l'industrie et le domaine énergétique : cela s'expliquait par un manque de formations disponibles sur le marché. Aujourd'hui, les propositions de formation initiale se sont étoffées, avec des écoles diplômantes en cybersécurité ou des cursus d'ingénieur spécialisés cyber. Le nombre d'ingénieurs, d'apprentis et de stagiaires sur le marché a crû, ce qui est une bonne nouvelle.

Ce qui manque, c'est la formation du management à un niveau plus élevé et l'acculturation au risque cyber dans les filières de formation continue. Selon moi, ce n'est pas aux industriels de la cyber de proposer ce niveau de formation, mais à la filière de la formation de s'adapter à cet enjeu. Des directives comme NIS 2 auront forcément un impact sur la demande, en raison des responsabilités importantes que devront assumer les cadres dirigeants.

La coconstruction public-privé d'offres et de solutions va de pair avec les sujets de politique industrielle que j'évoquais tout à l'heure. Se pose la question de la labellisation des offres, afin d'aider les nouveaux régulés à choisir des solutions en toute confiance quand ils n'ont pas forcément le bon niveau de maturité pour le faire.

La bonne nouvelle est que nous disposons de tous les vecteurs en France pour travailler sur les sujets. M. Guyonneau a mentionné le Comité de la filière industrielle de sécurité. Nous avons des fédérations professionnelles, comme l'Alliance pour la confiance numérique, qui sont des cadres d'échange pour les industriels et les offreurs : elles leur permettent de gérer les contraintes de compétition pour codévelopper des offres et des solutions.

L'ensemble des acteurs qui sont autour de la table aujourd'hui sont heureux, me semble-t-il, de participer à ces discussions.

M. Rémi Cardon. – Je serais curieux de connaître le coût d'investissement ou de fonctionnement – je ne sais pas comment vous le classez, car cela relève un peu des deux. Notre enjeu, c'est de convaincre de faire la bascule, et pour cela il est essentiel de disposer des chiffres clés. Il serait donc utile d'avoir une étude qualitative sur cet enjeu.

La directive doit être déclinée dans son pays, mais encore faut-il regarder les études d'impact. Certains d'entre vous se sont plaints du coût et de la concurrence déloyale. Comme vous disposez de plusieurs années d'ancienneté sur les enjeux cyber, avez-vous réfléchi à la question ? J'imagine que vous l'avez fait en interne, et le sujet est peut-être confidentiel.

Mme Catherine Morin-Desailly. – J'ai été sensible à la remarque consistant à dire qu'il était important que, concomitamment à cette nouvelle législation, une véritable politique industrielle soit mise en place. À quel niveau cette politique peut-elle être instaurée ? Faut-il profiter de la mise à

jour, prévue pour 2026, de la stratégie Décennie numérique, laquelle est largement insuffisante ?

Il faudrait prendre de nouvelles orientations et financer des solutions d'intelligence artificielle pour la cybersécurité et le quantique. Comment articuler cela avec les politiques nationales ?

M. Alexis Caurette. – Le sujet du cadre de l'exécution d'une politique industrielle est compliqué : on peut passer par différents véhicules. Je reste persuadé que l'Anssi peut s'occuper d'établir un recueil des besoins et d'émettre une feuille de route. L'Agence dispose de la liste des services et produits nécessaires pour accompagner l'exécution de la loi de programmation militaire : elle déploie des schémas de certification et de qualification des offres qui répondent à ces besoins. Nous avons un niveau d'exigence important du fait des enjeux de résilience de la Nation et de souveraineté, ce qui présente un risque de surcoût. Il faut trouver un moyen de « tamponner » les offres avec un visa de sécurité plus facile à atteindre, tout en garantissant la confiance et un bon niveau d'agilité.

Le risque derrière les offres qualifiées, c'est que, avec ce tampon, l'offre soit figée dans le temps jusqu'à son renouvellement. Dans la cybersécurité, il s'agit d'un réel problème ! Il faudrait disposer de modèles permettant d'avoir confiance dans les acteurs du conseil ou de la détection d'attaques sans leur imposer de tamponner une offre à un instant T et les empêcher de la faire évoluer dans le temps au risque de perdre leur tampon.

Sur le coût, je relayerai une remarque de Vincent Strubel, qui disait être étonné de voir des offres de conformité NIS 2 apparaître sur le marché du conseil alors qu'il n'avait pas encore travaillé sur les décrets d'application… Le coût de la mise en conformité dépendra des différents secteurs touchés et de ces décrets.

En tant qu'industriels, cela fait partie de nos politiques de produit que d'investir dans des offres et les développer. En ce qui concerne les entités régulées, quel sera, en fonction de leur point de départ, l'écart avec la conformité NIS 2 ? Pour les entreprises ou les organisations qui n'ont jamais rien fait, la marche sera haute ; d'autres, en revanche, ont déjà un certain niveau de maturité et d'éducation : elles devront peut-être adapter leur approche, mais le surcoût sera marginal.

Il est donc difficile de répondre à la question. Pour Vincent Strubel, le ticket d'entrée pour une entreprise de taille intermédiaire, qui n'aurait entrepris aucune démarche, est estimé à 200 000 euros.

M. Patrick Guyonneau. – En tant qu'OIV, nous avons des systèmes d'information d'importance vitale (SIIV), qui coûte 30 % plus cher qu'un système d'information (SI) normal, en raison des coûts de conception, de la maintenance dans de strictes conditions de sécurité et des coûts de supervision spécifiques parce qu'il faut un système de cloisonnement pour les logs.

Il faut que le SI régulé soit vraiment restreint aux entités importantes ou vitales. Les applications d'Orange pour le territoire national sont au nombre de 9 000, et nous avons quelques dizaines de SIIV – et le surcoût est déjà immense. La définition du périmètre est donc très importante : tout le monde ne peut se voir imposer les mêmes conditions de sécurité.

En ce qui concerne la politique industrielle, le comité stratégique de filière est aujourd'hui un peu endormi.

Mme Catherine Morin-Desailly. – Il faut le réveiller !

M. Patrick Guyonneau. – Plusieurs ministres doivent signer le contrat de filière.

M. Michaël Barthellemy. – La cybersécurité représente à peu près 10 % du coût d'un système d'information. Il ne faut pas se leurrer : chaque augmentation du niveau de sécurité se traduit soit par une hausse de l'enveloppe globale, au détriment de l'efficacité de l'entreprise, soit par une mise de côté de certaines exigences– la conformité n'est alors pas assurée.

Une flopée de consultants vous expliqueront les règles auxquelles il faut se conformer et celles qui se négocient. Il n'est pas étonnant qu'ils soient dès à présent un certain nombre sur le marché parce qu'ils regardent déjà comment biaiser par rapport à une loi qui n'est pas encore adoptée...

Les industriels, eux, vont demander à chacun de leurs fournisseurs dans leur chaîne d'approvisionnement d'apporter la preuve qu'ils se sont mis en conformité avec NIS 2. Pour être plus efficace, il faudrait qu'un organe puisse valider le niveau de conformité.

M. Olivier Cadic, président. – J'ai demandé à l'intelligence artificielle quel était le meilleur endroit en Europe pour être conforme à NIS 2 : j'ai obtenu une explication sur l'ISO 27000, et sur le fait qu'en la matière la Belgique était le pays le plus avancé aujourd'hui.

Pour le législateur, il est insupportable d'entendre que l'on doive s'en remettre à l'administration pour prendre un décret et nous dire comment les choses vont se passer. Car c'est nous qui sommes responsables devant les électeurs. Le bureau de notre commission spéciale prendra position sur la question, mais on ne peut pas s'en remettre à un organisme qui n'est pas soumis à un contrôle pour décider à quelle sauce nous allons être mangés…

Nous savons ce qu'il faut faire pour être conforme à NIS 2 puisque nous sommes allés à Bruxelles, où nous avons eu la réponse : il faut obtenir la norme ISO 27000 par un auditeur validé. Nous avons demandé à M. Strubel si un tel système serait accepté en France, et la réponse a été négative. Cela étant, un organisme qui obtient sa conformité NIS 2 en Belgique pourra intervenir sur notre territoire. Tout cela crée du trouble, et nécessite des clarifications.

Mes chers collègues, nous en avons terminé avec notre cycle d'auditions publiques.

Nous aurons ainsi pu, à notre niveau, contribuer à l'information des professionnels et du grand public avec : deux auditions de responsables publics – M. Vincent Strubel, directeur général de l'Anssi et Mme Clara Chappaz, ministre déléguée à l'intelligence artificielle et au numérique – ; et cinq tables rondes qui auront réuni les organisations professionnelles, des représentants des entreprises cyber, les associations d'élus, et aujourd'hui les autorités de régulation financière et trois grands acteurs de la cyberdéfense.

La réunion est close à 17 h 00.

Cette audition a fait l'objet d'une captation vidéo qui est disponible en ligne sur le site du Sénat.

II. EXAMEN DU RAPPORT

Mardi 4 mars 2025

M. Olivier Cadic, président. – Mes chers collègues, l'ordre du jour appelle l'examen du rapport de MM. Michel Canévet, Patrick Chaize et Hugues Saury sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Avant d'ouvrir la discussion, je voudrais vous remercier pour votre participation aux travaux de cette commission spéciale, qui aura surmonté une dissolution de l'Assemblée nationale et une censure gouvernementale, entre l'annonce du projet de loi initial pour juin 2024, le dépôt du texte le 15 octobre, et l'audition de la ministre, Mme Clara Chappaz, le 27 janvier dernier.

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 – M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), et Mme Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique ; et cinq tables rondes, avec les organisations professionnelles – Mouvement des entreprises de France (Medef), Confédération des petites et moyennes entreprises (CPME) –, des représentants des entreprises cyber – ACN, CyberCercle, CyberTaskForce, Clusif –, les associations d'élus – Association des maires de France et des présidents d'intercommunalité, Départements de France, Régions de France, Intercommunalités de France, métropole du Grand Paris –, les autorités de régulation financière – Autorité des marchés financiers (AMF) et Autorité de contrôle prudentiel et de résolution (ACPR) – et trois grands acteurs de la cyberdéfense – Airbus, Orange et Thales.

Ces auditions ont toutes été diffusées sur le site du Sénat et ont donné lieu à plus de 8 000 vues. En outre, elles ont fait l'objet de nombreuses reprises par les professionnels du secteur sur leurs réseaux sociaux. Cette séquence aura été notre contribution à une meilleure sensibilisation et à une meilleure information du public sur l'effort de résilience et de lutte contre les attaques cyber.

Je remercie également la commission des affaires européennes, présidée par notre collègue Jean-François Rapin, pour la communication qu'il a faite le 13 février dernier sur les dispositions de transposition et d'adaptation prévues par ce projet de loi – signe que ce texte mobilise le Sénat dans son ensemble. Ces observations ont été communiquées à l'ensemble des membres de notre commission spéciale.

Les rapporteurs ont également procédé à de nombreuses auditions. Avant de leur céder la parole pour vous présenter leurs principaux constats et

les orientations qu'ils préconisent sur le texte, j'ai deux précisions à vous apporter pour le bon déroulement de la réunion.

Je voudrais tout d'abord excuser notre collègue Patrick Chaize, qui a été retenu en Guyane et m'a demandé de bien vouloir lire son intervention et présenter ses amendements de concert avec les autres rapporteurs.

Ensuite, je vous rappelle qu'aura lieu, en séance, à seize heures trente, la déclaration du Gouvernement, suivie d'un débat, en application de l'article 50-1 de la Constitution, portant sur la situation en Ukraine et la sécurité en Europe. Aussi, je vous propose de nous fixer comme objectif de terminer d'ici là notre débat et l'examen des 124 amendements déposés sur ce texte, dont 53 émanent de nos rapporteurs.

M. Hugues Saury, rapporteur. – Je concentrerai mon intervention sur le titre Ier de ce projet de loi ainsi que sur les articles 5 et 6 du titre II, sur lesquels vous m'avez désigné rapporteur.

Le titre Ier vise à transposer en droit français la directive sur la résilience des entités critiques, dite « REC », qui fait suite à une première directive de 2008. 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.

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.

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 me 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.

Cette orientation me semble pertinente, car il est évident que l'on ne pourra jamais se protéger contre toutes les menaces. L'enjeu est donc bien d'identifier les moyens d'assurer la continuité des activités essentielles. Lors des auditions que j'ai menées, cette approche n'a d'ailleurs pas été remise en cause.

Par ailleurs, la directive REC vise désormais les « entités critiques » nationales, c'est-à-dire les opérateurs, et non plus seulement les infrastructures critiques européennes.

Pour ce qui concerne la transposition proprement dite, plusieurs différences doivent être signalées entre le texte qui nous est présenté et la directive. Les opérateurs « régaliens », c'est-à-dire exerçant dans le domaine de la défense ou de la sécurité nationale, qui étaient déjà soumis au dispositif de SAIV, sont ainsi intégrés dans le champ de la transposition, alors que cela n'était pas prévu par la directive.

Par ailleurs, la réalisation d'une analyse des dépendances à l'égard des tiers est prévue, alors que cette obligation ne figure pas dans la directive REC.

Enfin, les opérateurs d'importance vitale devront réaliser un plan de protection et de résilience pour chacun de leurs points d'importance vitale, comme cela est le cas dans le dispositif actuel, alors que la directive ne prévoit des plans qu'à l'échelle de l'opérateur lui-même.

Ces écarts à la directive REC me semblent cependant justifiés au regard de l'objectif poursuivi par le projet de loi, et je considère qu'il n'aurait pas été logique que des opérateurs régaliens restent soumis à un dispositif moins contraignant alors qu'ils exercent des activités par nature essentielles.

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

Tout d'abord, le champ d'application de la directive comprend 11 secteurs, contre 2 seulement – 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.

Ensuite, 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.

Enfin, un mécanisme de sanction administrative pouvant être prononcée par une commission des sanctions mise en place à cet effet est prévu en cas de manquement.

Sur ce dernier point, je me suis interrogé sur les plafonds de sanction inscrits dans le projet de loi, ces derniers étant élevés – 2 % du chiffre d'affaires ou 10 millions d'euros – et sensiblement plus importants que dans d'autres États membres.

Les directives REC et NIS 2 formant un ensemble cohérent et visant des objectifs convergents, il m'est cependant apparu justifié de prévoir des

niveaux de sanctions identiques. Il importe, en outre, que le régime de sanction soit dissuasif, même si la logique qui devra continuer de prévaloir doit être celle d'une collaboration étroite entre les opérateurs et l'administration.

Pour ce qui concerne l'article 1er, qui transpose la directive REC, j'ai déposé 14 amendements tendant notamment à apporter des modifications rédactionnelles, de précision ou de clarification ; à définir la notion d'« incident », laquelle emporte notamment l'obligation de notification que j'ai mentionnée tout à l'heure ; à définir la notion de « résilience », ce qui répond à une recommandation du Conseil d'État ; à préciser la date à partir de laquelle une astreinte prononcée dans le cadre d'une mise en demeure de réaliser, de modifier ou de mettre en œuvre un plan commence à s'appliquer ; à compléter l'analyse des dépendances à l'égard des tiers, en ne se limitant pas à la chaîne d'approvisionnement en matières premières, mais en intégrant également la chaîne de sous-traitance afin de réduire les « trous dans la raquette » ; à fixer à vingt-quatre heures le délai dans lequel l'opérateur doit signaler un incident à l'autorité administrative et à prévoir que le décret en Conseil d'État mentionné à l'alinéa 44 détermine l'ensemble des modalités de mise en œuvre de cette obligation, notamment pour la protection du secteur de la défense – ce décret pourra également préciser la nature des incidents devant être signalés à l'autorité administrative ; et à renforcer les garanties d'indépendance de la commission des sanctions, en prévoyant que les trois personnalités qualifiées qui y siégeront seront nommées non plus exclusivement par le Premier ministre, mais respectivement par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat.

La rédaction actuelle de l'article 4 me semble présenter une ambiguïté. Il existe un risque que les opérateurs d'importance vitale actuels voient leurs délais de mise en conformité réduits, car ils seront considérés comme OIV dès l'entrée en vigueur de la loi. Or il est évident que des textes d'application devront être pris ou à tout le moins actualisés, réduisant d'autant les délais fixés par le projet de loi. C'est pourquoi j'ai déposé un amendement visant à différer l'entrée en vigueur du titre Ier de manière à laisser le temps au Gouvernement de prendre l'ensemble des actes d'application nécessaire.

Sur le titre II, mes amendements visent à compléter la liste des définitions figurant à l'article 6, en particulier celles des notions d'« incident » et de « vulnérabilité », qui ne sont pas présentes dans le projet de loi alors qu'elles figurent dans la directive NIS 2.

M. Olivier Cadic, président, rapporteur, en remplacement de M. Patrick Chaize. – Permettez-moi de lire l'intervention de notre collègue rapporteur Patrick Chaize, qui vous prie de bien vouloir excuser son absence.

En sa qualité de rapporteur chargé de l'examen du titre II de ce projet de loi, et plus précisément de ses articles 7 à 42, son intervention sera centrée sur la transposition de la directive NIS 2.

Comme nos auditions nous l'ont clairement montré, au-delà de la hausse du nombre de secteurs et d'entités régulées, c'est un changement majeur de paradigme qui est à l'œuvre. Il s'agit non plus seulement, comme avec la directive NIS 1, de sécuriser des infrastructures critiques, mais aussi d'assurer la résilience de quelque 15 000 entités « essentielles » ou « importantes », en tant qu'organisations, et de l'ensemble de leurs systèmes d'information.

Bien évidemment, nous sommes, au Sénat, tout particulièrement sensibles à la situation des 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 – qui sont directement concernés par le présent projet de loi.

Pour en venir aux amendements qu'il vous propose d'adopter aujourd'hui, beaucoup d'entre eux visent à répondre au constat, largement partagé par les acteurs que nous avons entendus, d'une « sous-transposition » de la directive et d'un projet de loi de transposition « moins-disant », qui laisse une place trop importante aux dispositions de nature réglementaire.

Après l'article 5, il vous propose un amendement portant article additionnel prévoyant les grandes lignes de la stratégie nationale en matière de cybersécurité que devra élaborer le Premier ministre dans le nouveau contexte créé par NIS 2.

À l'article 7, qui renvoie intégralement à un décret en Conseil d'État la liste des secteurs « hautement critiques » et « critiques » concernés par le projet de loi, il vous propose un amendement visant à inscrire directement dans la loi les secteurs énumérés dans les annexes de la directive NIS 2. Afin de prévoir une certaine souplesse dans un domaine qui peut évoluer rapidement, un décret en Conseil d'État déterminera les sous-secteurs et les types d'entités relevant des secteurs.

À l'article 14, qui prévoit les obligations en matière de cybersécurité qui s'imposeront aux entités « essentielles » et « importantes », il vous propose un amendement, directement inspiré par la directive NIS 2, insistant sur la nécessaire proportionnalité de ces mesures : il convient de tenir compte systématiquement de la taille de l'entité, du degré de son exposition aux risques cyber, de la probabilité de survenance d'incidents et de leur gravité, afin de ne pas imposer des obligations excessives et trop coûteuses.

Au même article, un second amendement vient préciser, comme le fait la directive, que les décisions stratégiques en matière de cybersécurité doivent être prises par les organes de direction des entreprises ou des administrations publiques et que leurs dirigeants comme leurs personnels exposés aux risques cyber doivent être formés aux grands enjeux en matière de cybersécurité.

À l'article 17, qui concerne la procédure de notification des incidents, il vous propose plusieurs modifications destinées à mieux mettre en

conformité le texte du projet de loi avec celui de la directive. Il s'agit notamment de reprendre la définition d'« incident important » déclenchant une notification à l'Anssi, la définition proposée par la directive étant très claire ; de prévoir, conformément à la lettre de la directive NIS 2, une transmission, « sans retard injustifié », d'une « alerte précoce » dans un délai de « vingt-quatre heures » puis la transmission d'une « notification d'incident » dans un délai de « soixante-douze heures », puis la remise d'un rapport intermédiaire et d'un rapport final ; de prévoir que « l'autorité nationale de sécurité des systèmes d'information fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de la première notification reçue, une réponse à l'entité émettrice de la notification », puisque, de multiples obligations étant mises à la charge des entreprises et des administrations publiques, il est bon que, par symétrie, cette obligation mise par la directive à la charge de l'Anssi soit, elle aussi, prévue dans la loi ; de supprimer 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.

À l'article 29, il vous propose un amendement qui prévoit explicitement que l'entité faisant l'objet d'un contrôle de l'Anssi ne soit pas tenue de prendre en charge le coût du contrôle lorsque celui-ci ne révèle aucun manquement aux obligations qui s'imposent à elle. Il s'agit de préciser le cadre de l'exonération prévue par le texte déposé par le Gouvernement, qui accorde à l'Anssi un pouvoir discrétionnaire.

À l'article 35, il vous propose un amendement prévoyant que les personnalités qualifiées en matière de cybersécurité qui siégeront à la commission des sanctions devront ne pas avoir travaillé à l'Anssi depuis au moins cinq ans et seront nommées respectivement par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat, et non toutes par le Premier ministre.

À l'article 37, qui porte sur les sanctions applicables aux entités qui ne respecteraient pas les obligations prévues par le titre II transposant NIS 2, il vous propose de prévoir que la faculté, pour la commission des sanctions, d'interdire à une personne physique exerçant les fonctions de dirigeant dans une entité essentielle qui n'aurait pas accompli toutes ses obligations en matière de cybersécurité d'exercer des responsabilités dirigeantes dans cette entité est possible uniquement en dernier recours, si et seulement si le manquement persiste alors que l'entité essentielle s'est déjà vu imposer une amende administrative. Il s'agit de réserver cette sanction à des cas graves et exceptionnels qui verraient un dirigeant persister à refuser de résoudre un manquement alors même que son entreprise aurait déjà été sanctionnée.

Dans la perspective de la séance publique, il envisage de déposer des amendements aux articles 8 et 9 afin de 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.

Cette demande de l'Association des maires de France et des présidents d'intercommunalité me paraît raisonnable, mais il ne prévoit pas, en revanche, de retirer les communautés de communes du périmètre des entités régulées par le projet de loi.

Il avait également réfléchi à un mécanisme de crédit d'impôt destiné à aider les entreprises à financer leur mise au niveau de cybersécurité requis par NIS 2, mais le contexte de nos finances publiques lui apparaît beaucoup trop dégradé pour aller dans cette direction. Le Gouvernement travaille à 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. Il souhaiterait que nous puissions, en séance, sécuriser une accroche législative pour ce dispositif, afin de rassurer les entreprises sur ce point.

Enfin, il n'a pas, à ce stade, déposé d'amendement sur les délais d'application des mesures du titre II, malgré une demande très forte en ce sens des personnes que nous avons auditionnées, car la directive NIS 2 ne prévoit pas de tels délais. De ce fait, nous ne respecterions donc pas ses dispositions en les inscrivant dans la loi. Néanmoins, il déposera de tels amendements en séance, afin que le Gouvernement s'engage solennellement à ne pas appliquer les dispositions en matière de contrôle et de sanctions pendant au moins trois ans, voire davantage pour certaines entités.

Il faudra également, en séance, insister sur les efforts de communication et d'accompagnement que l'Anssi devra déployer pour que NIS 2 devienne une réalité concrète pour les 15 000 entités régulées.

M. Michel Canévet, rapporteur. – Il me revient d'aborder le titre III du projet de loi, qui transpose la directive DORA (*Digital Operational Resilience Act*) du 14 décembre 2022 et dont je suis le rapporteur. Cette directive modifie les directives sectorielles encadrant les secteurs bancaire, assurantiel et financier – à savoir la directive concernant les marchés d'instruments financiers (MIF 2), la directive sur les fonds propres réglementaires (CRD – *Capital Requirements Directive*), la directive Solvabilité II et la directive révisée sur les services de paiement (DSP 2) – pour prévoir que leur politique de gestion des risques liés aux technologies de l'information et de la communication (TIC) est conforme au règlement DORA du 14 décembre 2022.

S'agissant des entités financières identifiées en tant qu'entités essentielles ou importantes conformément aux dispositions nationales transposant l'article 3 de la directive NIS 2, le règlement DORA est considéré comme un acte juridique sectoriel de l'Union. Le paquet DORA constitue ainsi ce qu'on appelle la *lex specialis* de la directive NIS 2, c'est-à-dire sa déclinaison applicable au secteur financier.

Le secteur financier est, en effet, une cible de choix pour les cyberattaques : on peut, par exemple, rappeler que la filiale américaine de la banque chinoise ICBC a dû être recapitalisée à hauteur de plusieurs milliards

de dollars en 2024 à la suite d'une attaque par un rançongiciel. Le comité européen du risque systémique estime ainsi que le niveau élevé d'interconnexion dans le secteur financier 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. Les menaces cyber, en forte augmentation depuis plusieurs années, représentent ainsi, selon la Banque de France, un risque très élevé, supérieur au risque de marché et au risque climatique. Les cyberattaques peuvent ainsi être source de déstabilisation pour le système financier, exposé à une large gamme de risques TIC. En particulier, il faut noter que le recours fréquent à des prestations externes de services TIC étend la surface d'attaque des entités du secteur financier.

Une réglementation plus rigoureuse, permettant de sécuriser le système financier, mais aussi d'internaliser le coût de l'externalité négative que représente, du fait des interconnexions prévalant dans ce secteur, la défaillance d'une entité financière, était donc nécessaire, et c'est le sens du paquet DORA.

Le présent projet de loi précise les obligations qui s'imposent aux infrastructures de marché : les gestionnaires de plateformes de négociation doivent assurer et maintenir leur résilience opérationnelle conformément au règlement DORA – c'est l'objet de l'article 44 –, tandis que les entreprises de marché doivent gérer les risques liés aux TIC conformément aux exigences de ce règlement – c'est l'article 45. Il renforce également les obligations des établissements de crédit et des sociétés de financement, tant en termes de gouvernance qu'au regard des politiques d'urgence et de poursuite d'activité, mais aussi des plans de réponse et de rétablissement – articles 46 et 47 –, obligations auxquelles doivent également s'astreindre les prestataires de services d'investissement – articles 51 et 52. Les prestataires de services de paiement sont également ciblés – articles 48 et 49 –, de même que les entreprises d'assurance et de réassurance et les fonds de retraite professionnelle supplémentaire – article 57 –, les groupes d'assurance – article 58 –, les mutuelles et unions – article 59 – ainsi que les instituts de prévoyance et unions – article 61.

Il détermine également le rôle et les pouvoirs des autorités de supervision : l'article 53 s'attache à préciser que le secrétaire général de l'ACPR peut demander des renseignements à des prestataires tiers informatiques de personnes assujetties, tandis que l'article 54 complète le contenu des plans préventifs de résolution établis par le collège de résolution de l'ACPR de façon qu'ils puissent renforcer la résilience opérationnelle numérique de l'établissement supervisé.

Plusieurs sujets de préoccupation demeurent toutefois, dont seuls quelques-uns peuvent faire l'objet d'une modification législative au sein de ce projet de loi.

Je vous propose ainsi d'adopter, outre deux amendements rédactionnels, plusieurs amendements ayant pour principal objet de simplifier la vie des entreprises et d'éviter les différences de traitement entre elles.

Avant l'article 62, je vous proposerai d'adopter un amendement portant article additionnel destiné à éviter un double assujettissement à DORA et à NIS 2, dans la mesure où le respect des obligations que prévoit DORA est réputé valoir respect des obligations prévues par NIS 2.

Pour simplifier les démarches de « reporting », je vous propose deux amendements, l'un de rédaction globale de l'article 49, visant à fusionner les dispositifs de déclaration d'incidents opérationnels ou de sécurité liés au paiement prévus par la directive sur les services de paiement et le dispositif de déclaration d'incidents liés aux TIC prévu par le règlement DORA, et un article additionnel avant l'article 43, tendant à créer une sorte de « guichet unique », en désignant les autorités compétentes dans le cas d'une multiplicité d'autorités de supervision.

Je vous proposerai également un amendement portant article additionnel destiné à éviter des différences de traitement entre les entreprises d'investissement en prévoyant que le règlement DORA s'applique aux succursales d'entreprises d'investissement de pays tiers, conformément à l'approche traditionnellement retenue d'étendre les dispositions prudentielles pertinentes à ces succursales.

Enfin, je vous propose deux amendements destinés à éviter les surtranspositions ou, du moins, à en modérer les effets, en prévoyant, d'une part, à l'article 62, le report à 2030 de l'application du titre III à l'ensemble des sociétés de financement, puisque ces sociétés, de droit français, ne sont pas visées par le paquet DORA, et, d'autre part, la suppression de l'article 53, qui ajoute une précision superfétatoire et potentiellement contre-productive dans le code monétaire et financier, selon laquelle les prestataires tiers de services fondés sur les TIC figurent dans le périmètre du droit de communication dont dispose le secrétaire général de l'ACPR.

Au-delà de ce qu'il est possible de faire au sein du présent texte, il conviendra que l'ACPR et l'AMF prennent les dispositions nécessaires pour s'adapter à la nouvelle donne induite par DORA. Surtout, les normes techniques européennes de niveau 2 – normes techniques réglementaires (RTS – *Regulatory Technical Standards*) et normes techniques d'exécution (ITS – *Implementing Technical Standards*) – nécessaires à la pleine application des dispositions du paquet DORA n'ont pas toutes été prises : il y a là une urgence qu'il convient de souligner, car il importe que les acteurs puissent avoir connaissance de ces dispositions le plus vite possible afin de se mettre en conformité.

M. Olivier Cadic, président. – Mes chers collègues, il me revient à présent, en application du vade mecum sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, adopté par la Conférence des présidents,

de vous présenter le périmètre retenu pour juger de la recevabilité des amendements susceptibles de présenter un lien, même indirect, avec le texte déposé.

Ce périmètre comprend les dispositions relatives aux obligations qui s'imposent aux opérateurs désignés comme opérateurs d'importance vitale en matière de résilience de leurs activités d'importance vitale ; les dispositions relatives aux obligations qui s'imposent aux opérateurs désignés comme entités critiques d'importance européenne particulière en matière d'information de l'autorité administrative et, le cas échéant, d'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels dans le cadre d'une mission de conseil menée par la Commission européenne ; les dispositions relatives aux cas d'accès aux points d'importance vitale et systèmes d'information d'importance vitale et aux fonctions pouvant faire l'objet d'enquêtes administratives de sécurité à la demande des opérateurs ; les dispositions relatives au rôle et aux pouvoirs de l'autorité publique en matière de contrôle et de sanction des manquements aux obligations s'imposant aux opérateurs d'importance vitale ; les dispositions ayant trait aux marchés publics et contrats de concession relatifs à la sécurité des activités d'importance vitale ; les dispositions relatives aux missions de l'autorité nationale de sécurité des systèmes d'information ou des organismes qui jouent un rôle équivalent dans le domaine de la défense ; les dispositions qui s'imposent aux entreprises, aux établissements publics à caractère industriel et commercial, aux opérateurs de communications électroniques, aux prestataires de service de confiance, aux offices d'enregistrement, aux fournisseurs de services de systèmes de noms de domaine, aux administrations, aux collectivités territoriales et à leurs établissements publics et aux établissements d'enseignement menant des activités de recherche en matière de sécurité des systèmes d'information, de supervision de ces obligations par l'autorité nationale de sécurité des systèmes d'information et, le cas échéant, de sanction de leur méconnaissance ; les dispositions relatives au contrôle des moyens et prestations de cryptologie ; les dispositions relatives aux sanctions des activités prohibées susceptibles de brouiller les émissions hertziennes ; les dispositions relatives aux conditions d'accès à une assignation de fréquences déposée par la France auprès de l'Union internationale des télécommunications ; les dispositions relatives aux obligations qui s'imposent aux infrastructures de marché, aux établissements de crédit, aux sociétés de financement, aux prestataires de services d'investissement et de services de paiement, aux entreprises d'assurance et de réassurance, aux fonds de retraite professionnelle supplémentaire, aux groupes d'assurance, aux mutuelles, instituts de prévoyance et unions ainsi qu'à leurs prestataires tiers, en matière de gestion des risques liés aux technologies de l'information et de la communication ; les dispositions relatives au rôle et aux pouvoirs des autorités de supervision des secteurs bancaire, assurantiel et financier en matière de gestion des risques liés aux technologies de l'information et de la communication.

Il en est ainsi décidé.

Mme Catherine Morin-Desailly. – Je souscris aux analyses des rapporteurs. Il est essentiel de faire de la directive transposée une réussite opérationnelle et de veiller à harmoniser notre réglementation avec celle des autres pays européens. Nous devons travailler ensemble pour nous défendre, pour organiser la cybersécurité et pour construire une filière industrielle dans ce domaine.

Comme l'a dit l'un des rapporteurs, il faudra insister lors de l'examen du texte en séance sur l'effort de pédagogie que devra fournir l'Anssi auprès des entreprises et des collectivités territoriales. En effet, nous sommes nombreux à constater que nos collectivités sont encore loin d'être sensibilisées à ce sujet. Cela nécessite la mobilisation de moyens humains et financiers. Nous devons monter en compétence numérique et le Gouvernement devra se positionner clairement pour définir une stratégie globale.

En outre, malgré tous les règlements que nous pourrons faire, sans politique industrielle dédiée, nous ne pourrons pas assurer la cybersécurité. Il faut que ce texte contribue à ce que l'effet de ruissellement de cette filière industrielle soit correctement accompagné par la France et l'Europe.

Enfin, puisque j'ai l'honneur de représenter le Sénat à la Commission nationale de l'informatique et des libertés (Cnil), je précise que celle-ci se félicite de ce texte. La transposition de la directive incitera à étendre encore davantage le champ de la coopération entre la Cnil et l'Anssi pour créer un cadre cohérent. Certains points méritent d'être approfondis avant l'examen du texte en séance, pour éviter notamment les doublons en matière de sanctions.

Mme Audrey Linkenheld. – Les élus du groupe socialiste souscrivent largement aux constats qui viennent d'être dressés au sujet de la transposition de cette directive et aux améliorations que les rapporteurs proposeront au travers de leurs amendements.

Je vous avais parlé de la cyberattaque dont a été victime la ville de Lille et je vous avais exposé les enseignements que nous en avions tirés, notamment sur la nécessité d'accompagner les collectivités territoriales en amont aussi bien qu'en aval d'une éventuelle attaque.

Or deux ans à peine après cette attaque qui a eu des conséquences importantes, la chambre régionale des comptes a jugé pertinent de venir contrôler la ville de Lille, de sorte qu'un magistrat est venu commenter les mesures que nous avons prises et nous faire des recommandations. Il ne s'agit pas de contester le diagnostic d'ailleurs assez juste qu'il a fait, mais de vous faire part d'un certain étonnement face à cette démarche. En effet, comment peut-on demander aux collectivités de prendre des mesures et de définir des stratégies en matière de cyberprotection et de cyberrésilience, alors même que nous n'avons pas fini d'examiner ce texte au Sénat et qu'aucune stratégie n'a été définie à l'échelle nationale ?

Cela signifie que le texte issu de nos travaux sera examiné avec attention par ceux qui contrôlent les collectivités locales, et pas seulement par l'Anssi. Nous devrons donc nous montrer très vigilants.

EXAMEN DES ARTICLES

Article 1er

M. Hugues Saury, rapporteur. – Demande de retrait ou avis défavorable à l'amendement COM-10 qui vise à définir la notion d'incident. En effet, mieux vaut utiliser la terminologie nationale en utilisant les termes d'« activité d'importance vitale » plutôt que ceux de « service essentiel » comme le propose l'amendement des rapporteurs COM-82.

L'amendement COM-10 n'est pas adopté.

M. Hugues Saury, rapporteur. – Même avis sur l'amendement COM-11 qui vise à définir la notion de résilience. Demande de retrait au profit de l'amendement des rapporteurs COM-83.

L'amendement COM-11 n'est pas adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-31 vise à préciser la notion d'activité d'importance vitale en intégrant une référence à la santé publique et à l'environnement. Dans la mesure où ces éléments figurent dans la définition du service essentiel inscrite à l'article 2 de la directive REC, l'avis est favorable.

L'amendement COM-31 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-78 tend à définir les activités d'importance vitale numériques. Il n'est pas opportun de créer une telle catégorie spécifique, déjà incluse dans la notion générique d'activité d'importance vitale. Demande de retrait ou avis défavorable.

Mme Patricia Demas. – Je le retire.

L'amendement COM-78 est retiré.

M. Hugues Saury, rapporteur. – Notre amendement COM-81 est rédactionnel.

L'amendement COM-81 est adopté.

M. Hugues Saury, rapporteur. – Notre amendement COM-82 vise à définir l'incident comme « un événement qui perturbe ou est susceptible de perturber de manière importante l'exercice d'une activité d'importance vitale ». Nous voulons ainsi transposer l'article 2 de la directive européenne REC, en l'adaptant et en reprenant la terminologie nationale.

L'amendement COM-82 est adopté.

M. Hugues Saury, rapporteur. – Dans notre amendement COM-83, nous reprenons, en l'adaptant, la définition du terme « résilience » figurant à

l'article 2 de la directive européenne. La résilience est ainsi définie comme « la capacité d'un opérateur à prévenir et à se protéger contre tout incident, ainsi qu'à assurer la continuité de l'activité d'importance vitale qu'il exerce ».

L'amendement COM-83 est adopté.

M. Hugues Saury, rapporteur. – Avis défavorable à l'amendement COM-32 qui vise à instaurer une obligation de concertation préalable entre l'autorité administrative et l'opérateur concerné avant de le désigner opérateur d'importance vitale.

Si je partage l'intention des auteurs de cet amendement, le dispositif de résilience des activités d'importance vitale doit reposer sur un impératif d'efficacité qui implique une certaine rapidité. La procédure actuelle, qui devrait être reprise dans les textes d'application à venir, prévoit uniquement la possibilité pour l'opérateur de produire des observations. Il ne me semble pas opportun d'aller au-delà.

L'amendement COM-32 n'est pas adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-33 a pour objet de préciser le périmètre des entités pouvant être désignées comme opérateurs d'importance vitale. Il est satisfait par la rédaction actuelle de l'alinéa 13, qui dispose que sont désignés OIV « les opérateurs publics ou privés exerçant, au moyen d'infrastructures critiques situées sur le territoire national, une activité d'importance vitale ». Cette activité n'est donc pas exclusive de l'exercice d'une autre activité. Demande de retrait ou avis défavorable.

M. Mickaël Vallet. – Notre amendement vise surtout la question de la proportionnalité.

Mme Audrey Linkenheld. – Les obligations de l'OIV s'imposent-elles à une seule activité ou bien à toutes les activités ?

M. Hugues Saury, rapporteur. – Elles s'imposent à l'opérateur au titre de l'exercice d'une activité, le cas échéant, parmi d'autres.

M. Mickaël Vallet. – Il s'agit de trouver la meilleure rédaction possible. Nous pourrons en discuter en séance.

L'amendement COM-33 n'est pas adopté.

L'amendement de précision COM-84 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-34 vise à préciser les secteurs couverts par la directive REC. Il est satisfait par la rédaction actuelle de l'alinéa 14, qui dispose que l'autorité administrative peut mentionner « l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur de l'Union européenne définis par le règlement délégué de la Commission européenne ». Or ce règlement délégué fixe déjà une liste de secteurs et même de sous-secteurs devant être regardés comme des services essentiels. Demande de retrait ou avis défavorable.

L'amendement COM-34 n'est pas adopté.

L'amendement rédactionnel COM-85 *est adopté.*

M. Hugues Saury, rapporteur. – L'amendement COM-35 tend à préciser la nature des risques devant être évalués par les OIV. Il est satisfait par la rédaction actuelle de l'alinéa 20, qui prévoit que les OIV réalisent une analyse des risques « de toute nature, y compris à caractère terroriste », ce qui inclut donc ceux que mentionne l'amendement. Demande de retrait ou avis défavorable.

M. Mickaël Vallet. – Pourquoi préciser « y compris à caractère terroriste » s'il s'agit des risques « de toute nature » ?

M. Hugues Saury, rapporteur. – Parce qu'il s'agit d'un risque bien spécifique, qui nécessite des coordinations particulières, par exemple avec le plan Vigipirate.

M. Mickaël Vallet. – L'amendement est surtout rédactionnel, bien évidemment…

Mme Audrey Linkenheld. – Il ne vise qu'à transposer la directive.

L'amendement COM-35 est adopté.

L'amendement rédactionnel COM-86 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-36 qui a pour objet d'intégrer la notion de résilience dans les mesures prises par les OIV est satisfait par notre amendement COM-83, qui définit la résilience en y intégrant notamment la notion de prévention des incidents. Demande de retrait ou avis défavorable.

L'amendement COM-36 n'est pas adopté.

M. Hugues Saury, rapporteur. – Notre amendement COM-87 vise à clarifier la date à partir de laquelle une astreinte pécuniaire peut être imposée à l'opérateur mis en demeure de réaliser ou de modifier son plan de résilience opérateur.

L'amendement COM-87 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-37 vise à distinguer les éléments classifiés au sein du plan de résilience opérateur (PRO). Mais que signifie le terme de « distinguer » en droit ? Demande de retrait ou avis défavorable.

L'amendement COM-37 n'est pas adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-38 vise à renforcer l'identification des dépendances et interdépendances des opérateurs d'importance vitale. J'en demande le retrait au profit de mon amendement COM-88, dont la rédaction me semble plus claire.

L'amendement COM-38 n'est pas adopté.

M. Hugues Saury, rapporteur. – Notre amendement COM-88 vise à préciser que l'analyse des dépendances à l'égard de tiers ne se limite pas à leur chaîne d'approvisionnement, mais inclut également les sous-traitants qui peuvent constituer des points de vulnérabilité.

L'amendement COM-88 est adopté.

M. Hugues Saury, rapporteur. – Avis défavorable à l'amendement COM-39, car il est satisfait par la rédaction actuelle de l'alinéa 32, qui prévoit que les plans particuliers de résilience détaillent les mesures de protection et de résilience mises en œuvre.

M. Mickaël Vallet. – Je le retire.

L'amendement COM-39 est retiré.

M. Hugues Saury, rapporteur. – Notre amendement COM-89 a pour objet de clarifier la date à partir de laquelle une astreinte pécuniaire peut être imposée à un opérateur faisant l'objet d'une mise en demeure.

L'amendement COM-89 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-40 prévoit un avis préalable de la Cnil sur le décret en Conseil d'État fixant les modalités de mise en œuvre des enquêtes administratives de sécurité.

Je demande le retrait de cet amendement. Dans le cadre du dispositif de SAIV actuel, les enquêtes administratives de sécurité peuvent déjà donner lieu à la consultation du bulletin n° 2 du casier judiciaire ainsi que des traitements automatisés de données à caractère personnel.

Mme Audrey Linkenheld. – L'avis de la Cnil porte sur le décret, pas sur les enquêtes.

Mme Catherine Morin-Desailly. – L'avis de la Cnil a-t-il été sollicité sur ce sujet particulier ?

M. Hugues Saury, rapporteur. – J'invite les auteurs de cet amendement à le redéposer en séance afin d'entendre l'avis du Gouvernement, notamment sur cette dernière question. Demande de retrait ou avis défavorable.

M. Mickaël Vallet. – Nous le retirons.

L'amendement COM-40 est retiré.

M. Hugues Saury, rapporteur. – Notre amendement COM-90 rectifié prévoit, d'une part, que la notification d'incident doit intervenir au plus tard vingt-quatre heures après que l'opérateur en a pris connaissance, et, d'autre part, que le décret en Conseil d'État mentionné à l'alinéa 44 déterminera l'ensemble des conditions de mise en œuvre de cette obligation de notification.

Je demande le retrait de l'amendement COM-41 au profit de notre amendement COM-90 rectifié. Il me semble en effet préférable de ne pas détailler le contenu du décret en Conseil d'État pour permettre au pouvoir réglementaire d'établir,

par exemple, des exceptions liées à la protection du secret de la défense nationale et préciser la nature des incidents devant être signalés à l'autorité administrative.

L'amendement COM-90 rectifié est adopté. En conséquence, l'amendement COM-41 devient sans objet.

M. Hugues Saury, rapporteur. – Avis favorable à l'amendement COM-42 qui vise à définir les entités considérées comme critiques au niveau européen, en reprenant les critères de la directive REC.

L'amendement COM-42 est adopté, de même que l'amendement rédactionnel COM-91 .

M. Hugues Saury, rapporteur. – Avis favorable à l'amendement COM-43 qui vise à préciser utilement les conditions dans lesquelles une mission de conseil pourra être effectuée auprès d'une entité critique d'importance européenne particulière.

L'amendement COM-43 est adopté.

M. Hugues Saury, rapporteur. – Notre amendement COM-92 a pour objet d'étendre l'applicabilité du moyen de démontrer la conformité aux règles de sécurité aux opérateurs d'importance vitale qui ne sont soumis ni à la directive REC ni à la directive NIS 2.

L'amendement COM-92 est adopté.

M. Hugues Saury, rapporteur. – Notre amendement COM-93 vise à corriger une erreur matérielle.

L'amendement COM-93 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-44 prévoit de limiter les pouvoirs de contrôle des agents chargés de la supervision des OIV aux lieux à usage professionnel et aux lieux d'exécution d'une prestation de service en lien avec les installations sensibles.

J'y suis défavorable pour deux raisons. D'une part, il me semble que la restriction prévue par l'amendement est susceptible de priver l'accès à des locaux qui, bien que n'ayant pas de « lien avec les installations sensibles » peuvent présenter un intérêt majeur dans le cadre d'un contrôle : je pense par exemple au siège d'une entreprise. D'autre part, la notion d'installations sensibles est trop imprécise.

Mme Audrey Linkenheld. – Le « lien avec les installations sensibles » permettait d'inclure les sièges sociaux des entreprises.

M. Hugues Saury, rapporteur. – La rédaction actuelle le prévoit déjà.

Mme Audrey Linkenheld. – Nous souhaitions permettre que le contrôle se fasse jusqu'au bout sans pour autant aller trop loin dans les demandes faites à une entreprise privée.

M. Hugues Saury, rapporteur. – Nous pourrons en discuter en séance.

M. Mickaël Vallet. – Nous retirons notre amendement.

L'amendement COM-44 est retiré.

M. Hugues Saury, rapporteur. – L'amendement COM-45 est satisfait par l'alinéa 83 qui dispose déjà que les membres de la commission des sanctions « exercent leurs fonctions en toute impartialité » et que « dans l'exercice de leurs attributions, ils ne reçoivent ni ne sollicitent d'instruction d'aucune autorité ». Demande de retrait.

M. Mickaël Vallet. – Nous le retirons.

L'amendement COM-45 est retiré.

M. Hugues Saury, rapporteur. – Notre amendement COM-94 prévoit que les trois personnalités qualifiées qui siégeront à la commission des sanctions ne seront plus exclusivement nommées par le Premier ministre, mais, respectivement, par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat.

L'amendement COM-94 est adopté.

L'article 1er est adopté dans la rédaction issue des travaux de la commission.

Après l'article 1er

M. Hugues Saury, rapporteur. – Comme je l'ai déjà dit, il ne me semble pas opportun de créer une catégorie spécifique d'activités d'importance vitale numériques, celles-ci étant par nature comprises dans la notion générique d'activité d'importance vitale. Demande de retrait ou avis défavorable à l'amendement COM-79.

Mme Patricia Demas. – Je le retire.

L'amendement COM-79 est retiré.

M. Hugues Saury, rapporteur. – Même avis sur l'amendement COM-80, pour les mêmes raisons.

Mme Patricia Demas. – Je le retire.

L'amendement COM-80 est retiré.

Article 2

L'article 2 est adopté sans modification.

Article 3

L'article 3 est adopté sans modification.

Article 4

M. Hugues Saury, rapporteur. – L'amendement COM-95 a pour objet de différer l'entrée en vigueur du titre Ier à une date fixée par décret en Conseil d'État, au plus tard un an après la promulgation du texte.

L'amendement COM-95 est adopté.

L'article 4 est adopté dans la rédaction issue des travaux de la commission.

Article 5

M. Hugues Saury, rapporteur. – L'amendement COM-46 est satisfait par mon amendement COM-96 qui précise que l'Anssi est mentionnée à l'article L. 2321-1 du code de la défense. Aussi, je demande à ses auteurs de le retirer.

M. Mickaël Vallet. – Nous le retirons.

L'amendement COM-46 est retiré.

L'amendement de précision COM-96 est adopté.

M. Hugues Saury, rapporteur. – L'amendement COM-47 vise à préciser que l'Anssi est le point de contact unique pour les autorités compétentes des autres États membres, pour la Commission européenne et pour l'Agence européenne pour la cybersécurité (Enisa – *European Union Agency for Cybersecurity*).

Dès lors que l'Anssi est l'autorité unique chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information et de son contrôle, la précision apportée par cet amendement me semble superfétatoire. Avis défavorable.

L'amendement COM-47 n'est pas adopté.

M. Hugues Saury, rapporteur. – Il me semble opportun de préciser que les missions de l'Anssi comprennent l'accompagnement et le soutien au développement de la filière cybersécurité. Ces deux dimensions, pourtant primordiales, sont en effet absentes de ses missions actuelles. Avis favorable à l'amendement COM-58.

L'amendement COM-58 est adopté.

L'article 5 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 5

M. Olivier Cadic, président, rapporteur. – L'amendement COM-27 est largement satisfait par l'amendement COM-97 des rapporteurs qui prévoit l'élaboration d'une stratégie nationale en matière de cybersécurité. Cette stratégie devra bien sûr revenir en détail sur l'indispensable accompagnement des PME-TPE et des collectivités territoriales dans leur montée en maturité cyber. Demande de retrait ou avis défavorable.

Mme Audrey Linkenheld. – Nous le retirons même s'il n'est pas complètement satisfait. Nous pourrons en discuter en séance.

L'amendement COM-27 est retiré.

M. Olivier Cadic, président, rapporteur. – L'idée d'identifier un sous-préfet en qualité de référent en matière de cybersécurité par département est intéressante, mais je pense que c'est plutôt aux centres gouvernementaux de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) ou aux CSIRT (*Computer Security Incident Response Team*) régionaux de jouer le rôle d'animation de la cybersécurité au niveau local, sous l'égide de l'Anssi. Je demande le retrait de l'amendement COM-49.

Mme Audrey Linkenheld. – Les CSIRT ne dépendent pas de l'administration décentralisée. Leur rôle est d'intervenir en cas d'incident. Or nous voulons identifier dans l'administration décentralisée un appui susceptible d'accompagner les collectivités territoriales dans leur mise à niveau en matière de cybersécurité, ainsi que lors d'éventuels incidents, y compris sur des questions non numériques. Il s'agit d'améliorer l'accompagnement technique des collectivités.

M. André Reichardt. – Que propose le rapporteur pour appuyer les collectivités territoriales ?

M. Olivier Cadic, président, rapporteur. – Le rapporteur renvoie aux centres d'expertise et de ressources des titres (CERT) ou aux CSIRT. Une organisation existe déjà partiellement sous l'égide de l'Anssi. Il ne nous paraît pas opportun de confier cela au sous-préfet. Il sera intéressant d'entendre l'avis du Gouvernement sur le sujet.

M. André Reichardt. – Dans l'amendement, s'agit-il d'un sous-préfet en fonction ?

Mme Audrey Linkenheld. – Oui. Nous ne voulons pas créer de nouveau poste, mais identifier au sein de la préfecture un référent qui assurera la fonction cyber au niveau local, en complément des CSIRT.

Nous retirons notre amendement.

L'amendement COM-49 est retiré.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-97 vise à compenser l'absence de référence à une stratégie nationale de cybersécurité.

L'amendement COM-97 est adopté et devient article additionnel.

Article 6

M. Hugues Saury, rapporteur. – L'amendement COM-98 tend à reprendre la définition du terme « incident » telle qu'énoncée à l'article 6 de la directive NIS 2, à savoir « un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises

ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles ».

L'amendement COM-98 est adopté.

M. Hugues Saury, rapporteur. – Dans le même esprit, l'amendement COM-99 vise à définir la notion de vulnérabilité.

L'amendement COM-99 est adopté.

L'article 6 est adopté dans la rédaction issue des travaux de la commission.

Article 7

M. Olivier Cadic, président, rapporteur. – L'amendement COM-18 tend à renvoyer, pour la liste des secteurs hautement critiques et critiques en matière de cybersécurité, aux annexes de la directive NIS 2. Cet amendement est satisfait par l'amendement COM-100, qui prévoit d'inscrire cette liste directement dans la loi.

L'amendement COM-18 est retiré. L'amendement COM-100 est adopté.

L'article 7 est adopté dans la rédaction issue des travaux de la commission.

Article 8

M. Olivier Cadic, président, rapporteur. – Les amendements identiques COM-23, COM-51 et COM-64 portent sur le caractère cumulatif des critères de taille et de chiffre d'affaires par bilan. L'article 3 de la directive dispose que sont des entités « essentielles » les entités appartenant à un secteur « hautement critique » qui dépassent les plafonds applicables aux moyennes entreprises. Si les rapporteurs comprennent le choix de proposer une définition positive des critères de taille permettant d'établir si une entreprise est ou non une entité essentielle, ils ne peuvent que constater que le choix initial de faire référence dans l'article 3 de la directive à la définition de l'article 2 de l'annexe de la recommandation 2003/361/CE créée une grande confusion. En effet, celui-ci ne permet pas de savoir quelles sont les entreprises entités essentielles, mais seulement quelles sont les entreprises en deçà des seuils permettant de les qualifier d'essentielles. Il aurait été nettement préférable de proposer directement une définition positive comme le fait le projet de loi de transposition. Avis défavorable.

Mme Catherine Morin-Desailly. – Les auteurs de ces amendements partagent la préoccupation d'éviter la surtransposition. Nous comprenons les arguments du rapporteur, mais la question mérite une discussion approfondie.

M. Olivier Cadic, président, rapporteur. – Je vous demande de bien vouloir retirer ces amendements et de les représenter en séance publique, afin d'entendre les explications du Gouvernement.

Les amendements identiques COM-23, COM-51 et COM-64 sont retirés.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-66 vise à exclure de la liste des entités essentielles les communautés d'agglomération ne comprenant pas au moins une commune de 30 000 habitants et plus. Le projet de loi prévoit que les communautés d'agglomération et les communes de plus de 30 000 habitants sont des entités essentielles, tandis que les communautés de communes sont des entités importantes du point de vue de la cybersécurité. Le rapporteur est ouvert à l'idée de faire passer les communautés d'agglomération ne comprenant pas au moins une commune de 30 000 habitants et plus dans la catégorie des entités importantes, auxquelles s'appliquent des obligations moins contraignantes. Il souhaite toutefois faire le point au préalable avec les représentants des intercommunalités et renvoyer ce débat à la séance, d'où une demande de retrait.

L'amendement COM-66 est retiré.

L'article 8 est adopté sans modification.

Article 9

M. Olivier Cadic, président, rapporteur. – Le rapporteur demande le retrait des amendements identiques COM-24 et COM-52 et de l'amendement COM-65.

Les amendements identiques COM-24 et COM-52 et l'amendement COM-65 sont retirés, de même que l'amendement COM-67*.*

L'article 9 est adopté sans modification.

Articles 10 et 11

Les articles 10 et 11 sont successivement adoptés sans modification.

Article 12

M. Olivier Cadic, président, rapporteur. – L'amendement COM-101 prévoit la mise à jour au minimum tous les deux ans de la liste des entités régulées par le titre II du projet de loi transposant la directive NIS 2.

L'amendement COM-101 est adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-60 porte sur l'information des entités régulées au sujet de leur obligation de déclaration et de chiffrement des données transmises. En la matière, les efforts de communication de l'Anssi devront être accrus, car un certain nombre d'entreprises ou de collectivités territoriales ne savent pas qu'elles seront éligibles à NIS 2 à l'issue de l'adoption de ce projet de loi. Il ne paraît pas toutefois nécessaire d'inscrire dans la loi cet impératif de communication et d'information, dont l'Anssi semble avoir pleinement conscience. En ce qui concerne l'obligation de chiffrement et la protection des données recueillies des lois extraterritoriales, l'Anssi devra naturellement prendre toutes les

mesures nécessaires. Que des données fuitent lors des échanges que l'Anssi entretiendra avec les entités régulées serait un comble ! M. Chaize partage l'objectif poursuivi, mais juge préférable de laisser l'Anssi prévoir elle-même les modalités de sécurisation de ces canaux de communication avec les entités régulées. Je demande donc le retrait de cet amendement.

L'amendement COM-60 est retiré.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-20 prévoit un avis de la Cnil sur le décret en Conseil d'État définissant les informations à transmettre pour l'application de l'article 12. Le rapporteur est favorable à cet amendement, dans la mesure où les informations transmises pourraient effectivement contenir des données personnelles.

L'amendement COM-20 est adopté.

L'article 12 est adopté dans la rédaction issue des travaux de la commission.

Article 13

M. Olivier Cadic, président, rapporteur. – L'amendement COM-61 prévoit une information régulière des entités par l'Anssi sur la réglementation qu'elles doivent respecter en matière de cybersécurité. L'article 13 vise à assurer la conciliation entre la transposition de la directive NIS 2, qui s'applique à tous les secteurs de l'économie, et le règlement et la directive DORA, qui constituent une *lex specialis* propre aux secteurs bancaire et financier. Il ne paraît donc pas nécessaire – cela serait lourd par ailleurs pour l'Anssi – de prévoir une information régulière des 15 000 entités régulées par NIS 2. Ces dernières sauront rapidement quelles règles elles devront respecter, seules les banques, les assurances ou les entreprises du secteur financier étant concernées par DORA. Je demande donc le retrait de cet amendement.

L'amendement COM-61 est retiré.

L'article 13 est adopté sans modification.

Article 14

M. Olivier Cadic, président, rapporteur. – L'amendement COM-15 tend à exiger la proportionnalité des mesures de cybersécurité qui sont imposées aux entités régulées. Retrait de cet amendement au profit de l'amendement COM-103.

L'amendement COM-15 est retiré.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-102 vise à rendre obligatoires l'approbation et la supervision des mesures de cybersécurité par les organes de direction des entités régulées.

L'amendement COM-102 est adopté.

M. Olivier Cadic, président, rapporteur. – L'article 14 prévoit que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent. On ne va pas demander, comme le proposent les auteurs de l'amendement COM-29, à chacune des 15 000 entités régulées au titre de NIS 2 de prendre des mesures destinées à « garantir les impératifs de souveraineté, de sécurité nationale, d'autonomie stratégique et de protection des réseaux contre les ingérences étrangères et les législations à portée extraterritoriale ». Toutefois, prises dans leur ensemble, les mesures portées par NIS 2 et par son projet de loi de transposition visent bien cet objectif au niveau macroéconomique, d'où une demande de retrait.

L'amendement COM-29 n'est pas adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-62 tend à prévoir la consultation des professionnels du secteur avant l'adoption du décret déterminant les caractéristiques du référentiel applicable aux entités régulées. Cet amendement n'apparaît pas nécessaire, car les représentants de la filière cyber sont déjà étroitement associés aux travaux de l'Anssi, notamment à l'élaboration de ce référentiel.

L'amendement COM-62 n'est pas adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-30 tend à créer un comité de suivi afin d'associer les représentants de la filière cyber et les représentants des entités concernées à l'élaboration du référentiel d'exigences techniques et organisationnelles pour la conformité à NIS 2. L'Anssi a indiqué que les exigences de ce référentiel s'inscriront dans la suite logique de l'actuelle réglementation NIS 1 et porteront principalement sur des aspects d'hygiène informatique fondamentale, afin que les entités puissent se protéger contre les menaces les plus courantes. Les représentants des entités concernées sont d'ores et déjà étroitement associés à la préparation de ce référentiel. Si le rapporteur partage la vigilance des auteurs de cet amendement et leur volonté de bien associer les représentants des entités régulées, la création d'un comité de suivi ne lui paraît pas nécessaire, la concertation étant déjà une réalité qui devra pleinement se poursuivre. Demande de retrait.

Mme Audrey Linkenheld. – Cela va sans dire, mais cela va tout de même mieux en le disant. Nous maintenons cet amendement.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-16 porte sur la proportionnalité des obligations imposées par le référentiel de l'Anssi aux entités régulées. D'où la demande de retrait au profit de l'amendement COM-103.

L'amendement COM-30 n'est pas adopté. L'amendement COM-16 est retiré. L'amendement COM-103 est adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-28 vise à créer un crédit d'impôt en faveur des PME pour leurs dépenses de cybersécurité. Sur cette question, je vous renvoie aux propos du rapporteur, qui a lui-même hésité à présenter un amendement de ce type. Le Gouvernement travaille à une forme de labellisation NIS 2, qui permettrait aux entreprises de valoriser leurs efforts en matière de cybersécurité auprès des banques notamment. Cette piste paraît devoir être explorée en priorité dans un contexte d'argent public devenu très rare.

L'amendement COM-28 n'est pas adopté.

L'article 14 est adopté dans la rédaction issue des travaux de la commission.

Article 15

M. Olivier Cadic, président, rapporteur. – L'amendement COM-104 vise à créer un mécanisme de reconnaissance mutuelle entre les États membres de l'Union européenne et vers d'autres types de référentiels.

L'amendement COM-104 est adopté.

L'article 15 est adopté dans la rédaction issue des travaux de la commission.

Article 16

L'amendement rédactionnel COM-105 *est adopté.*

L'article 16 est adopté dans la rédaction issue des travaux de la commission.

Article 17

M. Olivier Cadic, président, rapporteur. – L'amendement COM-12 prévoit une notification à l'Anssi dans un délai de vingt-quatre heures en cas d'incident important. Cet amendement est satisfait par l'amendement COM-106, d'où une demande de retrait.

Les amendements COM-12 et COM-26 *sont retirés.*

L'amendement COM-106 est adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-68, qui vise à préciser les délais de notification aux destinataires des services, ainsi que l'amendement COM-53 sont satisfaits par l'amendement COM-106, d'où une demande de retrait.

Les amendements COM-68 et COM-53 sont retirés.

L'article 17 est adopté dans la rédaction issue des travaux de la commission.

Articles 18, 19, 20, 21 et 22

Les articles 18, 19, 20, 21 et 22 sont successivement adoptés sans modification.

Article 23

M. Olivier Cadic, président, rapporteur. – Les amendements identiques COM-54 et COM-70 tendent à apporter des précisions utiles pour restreindre au strict nécessaire les informations échangées par l'Anssi avec ses différents partenaires. Avis favorable.

Les amendements identiques COM-54 et COM-70 sont adoptés.

L'article 23 est adopté dans la rédaction issue des travaux de la commission.

Article 24

L'article 24 est adopté sans modification.

Article 25

M. Olivier Cadic, président, rapporteur. – L'amendement COM-107 est rédactionnel. L'amendement COM-14 vise à préciser que les mesures pouvant être prescrites par l'Anssi en cas de menace pour la sécurité des systèmes d'information d'une entité doivent avoir un caractère adapté et proportionné. Demande de retrait, car, par définition, des mesures nécessaires ne peuvent être ni inadaptées ni disproportionnées. Du reste, cet amendement est incompatible avec l'amendement COM-107.

L'amendement COM-107 est adopté. L'amendement COM-14 n'est pas adopté.

L'article 25 est adopté dans la rédaction issue des travaux de la commission.

Avant l'article 26

L'amendement de coordination COM-108 *est adopté et devient article additionnel.*

Article 26

M. Olivier Cadic, président, rapporteur. – L'amendement COM-109 vise à supprimer la référence à certaines infractions et à clarifier le rôle des agents et personnels des organismes indépendants en matière de recherche de manquements. Il tend également à améliorer la qualité rédactionnelle du dispositif.

L'amendement COM-109 est adopté.

L'article 26 est adopté dans la rédaction issue des travaux de la commission.

Article 27

L'amendement rédactionnel et de sécurisation juridique COM-110 *est adopté.*

M. Olivier Cadic, président, rapporteur. – L'amendement COM-71 tend à restreindre l'accès des agents et des personnels chargés du contrôle aux systèmes d'information, logiciels, programmes informatiques et données stockées par l'entité contrôlée. Il ne s'agit là que d'une simple faculté accordée à ces agents et personnels parmi celles que liste l'article 27. En tout état de cause, il est nécessaire que ceux-ci accèdent à ces éléments, et notamment aux systèmes d'information, dans la mesure où le contrôle qu'ils mènent porte précisément sur le niveau de sécurité de ces systèmes d'information. Cet accès est directement nécessaire à l'accomplissement de leur mission. Demande de retrait.

L'amendement COM-71 est retiré.

L'article 27 est adopté dans la rédaction issue des travaux de la commission.

Article 28

M. Olivier Cadic, président, rapporteur. – Afin de sécuriser juridiquement le dispositif, l'amendement COM-111 vise à préciser le chiffre d'affaires retenu pour la détermination du plafond de l'amende prévue en cas d'obstacle au contrôle.

L'amendement COM-111 est adopté. En conséquence, les amendements COM-25, COM-56 *et* COM-72 *deviennent sans objet.*

M. Olivier Cadic, président, rapporteur. – L'amendement COM-55 tend à limiter le champ d'application de l'amende administrative pour obstacle au contrôle aux cas d'obstacle délibéré. Si le rapporteur partage l'intention de notre collègue Catherine Morin-Desailly, il serait difficile, pour un contrôleur, de déterminer si l'entité contrôlée a fourni des renseignements incomplets ou inexacts de manière délibérée ou si cette défaillance résulte de circonstances indépendantes de sa volonté. Dans le doute, la précision proposée atténuerait le caractère répressif du dispositif et ne contribuerait pas à inciter les entités contrôlées à répondre de bonne foi aux demandes qui leur sont adressées par les agents et personnels chargés du contrôle. L'amende administrative prévue en cas d'obstacle au contrôle doit être prononcée par la commission des sanctions sur saisine de l'Anssi. Par conséquent, dans le cas où celle-ci s'apercevrait que certains des renseignements fournis par l'entité contrôlée sont incomplets ou inexacts, il lui serait tout à fait possible de solliciter le complément d'information ou la rectification requis avant de saisir la commission des sanctions. Elle pourrait ainsi juger de la bonne foi de l'entité. Pour toutes ces raisons, je demande le retrait de cet amendement.

L'amendement COM-55 est retiré.

L'article 28 est adopté dans la rédaction issue des travaux de la commission.

Article 29

M. Olivier Cadic, président, rapporteur. – L'amendement COM-21 porte sur le choix par l'entité contrôlée de l'organisme chargé des audits de sécurité réguliers et ciblés. Ce dernier pourrait être soit l'Anssi, soit un organisme indépendant choisi par l'entité parmi les organismes agréés par l'Anssi. Le fait de permettre à l'entité contrôlée de choisir son contrôleur fragiliserait la fiabilité, l'efficacité et l'utilité du contrôle, en induisant un doute sur l'impartialité du contrôleur. Demande de retrait.

Mme Audrey Linkenheld. – Je maintiens cet amendement. Lesdits organismes étant agréés à cet effet par un tiers, je ne vois pas en quoi il peut y avoir un doute sur leur impartialité.

L'amendement COM-21 n'est pas adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-112 tend à apporter une clarification juridique quant à la prise en charge du coût des contrôles.

L'amendement COM-112 est adopté. En conséquence, l'amendement COM-17 *devient sans objet.*

L'article 29 est adopté dans la rédaction issue des travaux de la commission.

Article 30

M. Olivier Cadic, président, rapporteur. – L'amendement COM-19 vise une mise en œuvre progressive et différenciée des dispositions relatives aux prérogatives de l'Anssi en matière de recherche et de constatation des manquements. Comme la directive, le projet de loi ne fixe pas de date d'entrée en vigueur de ses dispositions. Néanmoins, il est prévu que ces dernières soient appliquées de façon progressive, certaines d'entre elles devant par exemple être mises en œuvre dans l'année, tandis que la ministre et le directeur général de l'Anssi se sont engagés, lors de leur audition, à ce que les premiers contrôles découlant du futur cadre législatif ne soient pas diligentés avant trois ans au moins. Cet amendement étant satisfait, j'en demande le retrait.

Mme Audrey Linkenheld. – Je reconnais qu'un certain nombre d'engagements oraux ont été pris. Néanmoins, je maintiens mon amendement de façon qu'ils soient inscrits dans la loi.

L'amendement COM-19 n'est pas adopté.

L'article 30 est adopté sans modification.

Article 31

M. Olivier Cadic, président, rapporteur. – L'amendement COM-113 a pour objet d'intégrer les dispositions de l'article 32 à l'article 31, de fixer les conditions d'ouverture d'une procédure à l'encontre de la personne contrôlée et de supprimer la faculté de publicisation des manquements et des mesures

d'exécution adoptées accordée à l'Anssi. Il s'agit notamment d'enjoindre à la personne contrôlée de rendre public son manquement. Seule la commission des sanctions serait donc habilitée à décider d'une mesure de publicisation, dans la mesure où celle-ci constitue davantage une sanction qu'une mesure de police administrative.

L'amendement COM-113 est adopté.

L'article 31 est adopté dans la rédaction issue des travaux de la commission.

Article 32

M. Olivier Cadic, président, rapporteur. – Dans un souci de simplification, l'amendement COM-114 vise à supprimer l'article 32, intégré par voie d'amendement à l'article précédent.

L'amendement COM-114 est adopté. En conséquence, les amendements COM-75, COM-76 *et* COM-74 *deviennent sans objet.*

L'article 32 est supprimé.

Article 33

L'amendement rédactionnel et de coordination COM-115 *est adopté. En conséquence, l'amendement* COM-22 *devient sans objet.*

L'article 33 est adopté dans la rédaction issue des travaux de la commission.

Article 34

L'article 34 est adopté sans modification.

Article 35

L'amendement de précision COM-116 *est adopté.*

L'article 35 est adopté dans la rédaction issue des travaux de la commission.

Article 36

L'amendement de précision rédactionnelle COM-117 *est adopté.*

M. Olivier Cadic, président, rapporteur. – L'amendement COM-118 prévoit la nomination des trois personnalités qualifiées en matière de cybersécurité respectivement par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat.

L'amendement COM-118 est adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-119 vise à interdire la nomination comme membre de la commission des sanctions d'une personnalité qualifiée ayant exercé des fonctions à l'Anssi depuis moins de cinq ans.

L'amendement COM-119 est adopté.

L'article 36 est adopté dans la rédaction issue des travaux de la commission.

Article 37

M. Olivier Cadic, président, rapporteur. – L'amendement COM-57, qui tend à préciser que l'interdiction aux personnes physiques exerçant des fonctions de dirigeant d'exercer des responsabilités n'est prise qu'en dernier recours, est satisfait par l'amendement COM-120, d'où une demande de retrait.

L'amendement COM-57 est retiré.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-77 est également satisfait par l'amendement COM-120.

L'amendement COM-77 est retiré.

L'amendement COM-120 est adopté.

M. Olivier Cadic, président, rapporteur. – L'amendement COM-121 porte sur la communication de la sanction imposée à une entité manquant à ses obligations en matière de cybersécurité au public.

L'amendement COM-121 est adopté.

L'article 37 est adopté dans la rédaction issue des travaux de la commission.

Article 38

L'article 38 est adopté sans modification.

Article 39

L'amendement rédactionnel COM-122 *est adopté.*

L'article 39 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 39

M. Olivier Cadic, président, rapporteur. – L'amendement COM-63 vise à mentionner la sécurisation des outils numériques dans un article du code du travail relatif aux conditions et à l'aménagement du poste de travail des travailleurs. Il est difficile de raccrocher directement cette question à la cybersécurité, d'où une demande de retrait.

Mme Catherine Morin-Desailly. – En l'absence du rapporteur, le débat est limité. Je retirerai donc mon amendement en séance.

L'amendement COM-63 n'est pas adopté.

Article 40

M. Olivier Cadic, président, rapporteur. – L'amendement COM-123 vise à clarifier l'applicabilité en Nouvelle-Calédonie et en Polynésie française des dispositions du présent projet de loi en matière de noms de domaine.

L'amendement COM-123 est adopté.

L'article 40 est adopté dans la rédaction issue des travaux de la commission.

Article 41

L'amendement rédactionnel COM-124 est adopté.

L'article 41 est adopté dans la rédaction issue des travaux de la commission.

Article 42

L'amendement de précision COM-125 est adopté.

L'article 42 est adopté dans la rédaction issue des travaux de la commission.

Avant l'article 43

M. Michel Canévet, rapporteur. – L'amendement COM-126 vise à désigner explicitement l'APCR comme interlocutrice unique de l'ensemble des institutions financières, sauf pour les dépositaires centraux, pour lesquels l'interlocutrice sera la Banque de France. Il s'agit d'éviter aux entreprises de devoir faire des déclarations auprès de plusieurs administrations.

L'amendement COM-126 est adopté et devient article additionnel.

Articles 43 et 44

Les articles 43 et 44 sont successivement adoptés sans modification.

Article 45

L'amendement rédactionnel COM-127 *est adopté.*

L'article 45 est adopté dans la rédaction issue des travaux de la commission.

Articles 46, 47 et 48

Les articles 46, 47 et 48 sont successivement adoptés sans modification.

Article 49

M. Michel Canévet, rapporteur. – L'amendement COM-128 vise à répercuter en droit français la fusion des dispositifs de déclarations d'incidents prévus par le règlement DORA et par la DSP2. Il est précisé que la Caisse des dépôts et consignations sera soumise aux obligations de notification.

L'amendement COM-128 est adopté.

L'article 49 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 49

M. Michel Canévet, rapporteur. – L'amendement COM-129 vise à étendre l'application du règlement DORA aux succursales d'entreprises d'investissement de pays tiers.

L'amendement COM-128 est adopté et devient article additionnel.

Articles 50, 51 et 52

Les articles 50, 51 et 52 sont successivement adoptés sans modification.

Article 53

M. Michel Canévet, rapporteur. – L'amendement COM-130 vise à supprimer l'article 53, qui donne des pouvoirs d'investigation au secrétaire général de l'ACPR. Cet article est satisfait par les textes existants.

L'amendement COM-130 est adopté.

L'article 53 est supprimé.

Articles 54 et 55

Les articles 54 et 55 sont successivement adoptés sans modification.

Article 56

L'amendement de correction COM-131 *est adopté.*

L'article 56 est adopté dans la rédaction issue des travaux de la commission.

Articles 57 et 58

Les articles 57 et 58 sont successivement adoptés sans modification.

Après l'article 58

M. Michel Canévet, rapporteur. – L'amendement COM-69 a pour objet de modifier très fortement le code des assurances en inversant la charge de la preuve.

Mme Vanina Paoli-Gagin. – Les dispositions actuelles nuisent au développement de l'assurance cyber en France. Partout ailleurs en Europe, la charge de la preuve revient à l'assureur.

M. Michel Canévet, rapporteur. – Je partage votre objectif. Toutefois, l'adoption de cet amendement conduirait à modifier le code de l'assurance bien au-delà du périmètre de ce texte. Il faudrait le circonscrire aux questions de cybersécurité.

L'amendement COM-69 est déclaré irrecevable en application de l'article 45 de la Constitution.

Articles 59, 60 et 61

Les articles 59, 60 et 61 sont successivement adoptés sans modification.

Avant l'article 62

M. Michel Canévet, rapporteur. – L'amendement COM-132 vise à préciser explicitement que les institutions financières sont soumises non pas aux dispositions de NIS 2, mais à celles de DORA.

L'amendement COM-132 est adopté et devient article additionnel.

Article 62

M. Michel Canévet, rapporteur. – L'amendement COM-133 vise à reporter l'entrée en vigueur des dispositions du titre III au lendemain de la promulgation de la loi. Pour les sociétés de financement pour lesquelles il y a une évidente surtransposition, je propose en revanche de repousser l'entrée en vigueur des articles 46, 47 et 54 non pas au 1er janvier 2026, mais au 1er janvier 2030.

L'amendement COM-133 est adopté.

L'article 62 est adopté dans la rédaction issue des travaux de la commission.

Le projet de loi est adopté dans la rédaction issue des travaux de la commission.

La réunion est close à 16 h 35.

RÈGLES RELATIVES À L'APPLICATION DE L'ARTICLE 45 DE LA CONSTITUTION ET DE L'ARTICLE 44 BIS DU RÈGLEMENT DU SÉNAT

Si le premier alinéa de l'article 45 de la Constitution, depuis la révision du 23 juillet 2008, dispose que « tout amendement est recevable en première lecture dès lors qu'il présente un lien, même indirect, avec le texte déposé ou transmis », le Conseil constitutionnel estime que cette mention a eu pour effet de consolider, dans la Constitution, sa jurisprudence antérieure, reposant en particulier sur « la nécessité pour un amendement de ne pas être dépourvu de tout lien avec l'objet du texte déposé sur le bureau de la première assemblée saisie » [1].

De jurisprudence constante et en dépit de la mention du texte « transmis » dans la Constitution, le Conseil constitutionnel apprécie ainsi l'existence du lien par rapport au contenu précis des dispositions du texte initial, déposé sur le bureau de la première assemblée saisie[2]. Pour les lois ordinaires, le seul critère d'analyse est le lien matériel entre le texte initial et l'amendement, la modification de l'intitulé au cours de la navette restant sans effet sur la présence de « cavaliers » dans le texte[3]. Pour les lois organiques, le Conseil constitutionnel ajoute un second critère : il considère comme un « cavalier » toute disposition organique prise sur un fondement constitutionnel différent de celui sur lequel a été pris le texte initial[4].

En application des articles 17 bis et 44 bis du Règlement du Sénat, il revient à la commission saisie au fond de se prononcer sur les irrecevabilités résultant de l'article 45 de la Constitution, étant précisé que le Conseil constitutionnel les soulève d'office lorsqu'il est saisi d'un texte de loi avant sa promulgation.

En application du vademecum sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, adopté par la Conférence des Présidents, la commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité a arrêté, lors de sa réunion du mardi 4 mars 2025, le périmètre indicatif du projet de loi n° 33

---

[1] *Cf. commentaire de la décision n° 2010-617 DC du 9 novembre 2010 - Loi portant réforme des retraites.*

[2] *Cf. par exemple les décisions n° 2015-719 DC du 13 août 2015 - Loi portant adaptation de la procédure pénale au droit de l'Union européenne et n° 2016-738 DC du 10 novembre 2016 - Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias.*

[3] *Décision n° 2007-546 DC du 25 janvier 2007 - Loi ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique.*

[4] *Décision n° 2020-802 DC du 30 juillet 2020 - Loi organique portant report de l'élection de six sénateurs représentant les Français établis hors de France et des élections partielles pour les députés et les sénateurs représentant les Français établis hors de France.*

(2024-2025). Sont susceptibles de présenter un lien, même indirect, avec le texte déposé :

- les dispositions relatives aux obligations qui s'imposent aux opérateurs désignés comme opérateurs d'importance vitale en matière de résilience de leurs activités d'importance vitale ;

- les dispositions relatives aux obligations qui s'imposent aux opérateurs désignés comme entités critiques d'importance européenne particulière en matière d'information de l'autorité administrative et, le cas échéant, d'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels dans le cadre d'une mission de conseil menée par la Commission européenne ;

- les dispositions relative aux cas d'accès aux points d'importance vitale et systèmes d'information d'importance vitale et aux fonctions pouvant faire l'objet d'enquêtes administratives de sécurité à la demande des opérateurs ;

- les dispositions relatives au rôle et aux pouvoirs de l'autorité publique en matière de contrôle et de sanction des manquements aux obligations s'imposant aux opérateurs d'importance vitale ;

- les dispositions ayant trait aux marchés publics et contrats de concession relatifs à la sécurité des activités d'importance vitale ;

- les dispositions relatives aux missions de l'autorité nationale de sécurité des systèmes d'information ou des organismes qui jouent un rôle équivalent dans le domaine de la défense ;

- les dispositions qui s'imposent aux entreprises, aux établissements publics à caractère industriel et commercial, aux opérateurs de communications électroniques, aux prestataires de service de confiance, aux offices d'enregistrement, aux fournisseurs de services de systèmes de noms de domaine, aux administrations, aux collectivités territoriales et à leurs établissements publics et aux établissement d'enseignement menant des activités de recherche en matière de sécurité des systèmes d'information, de supervision de ces obligations par l'autorité nationale de sécurité des systèmes d'information et, le cas échéant, de sanction de leur méconnaissance ;

- les dispositions relatives au contrôle des moyens et prestations de cryptologie ;

- les dispositions relatives aux sanctions des activités prohibées susceptibles de brouiller les émissions hertziennes ;

- les dispositions relatives aux conditions d'accès à une assignation de fréquences déposée par la France auprès de l'Union internationale des télécommunications ;

- les dispositions relatives aux obligations qui s'imposent aux infrastructures de marchés, aux établissements de crédit, aux sociétés de financement, aux prestataires de services d'investissement et de services de

paiement, aux entreprises d'assurance et de réassurance, aux fonds de retraite professionnelle supplémentaire, aux groupes d'assurances, aux mutuelles, instituts de prévoyance et unions, ainsi qu'à leurs prestataires tiers, en matière de gestion des risques liés aux technologies de l'information et de la communication ;

- les dispositions relatives au rôle et aux pouvoirs des autorités de supervision des secteurs bancaire, assurantiel et financier en matière de gestion des risques liés aux technologies de l'information et de la communication.

LISTE DES PERSONNES ENTENDUES

I. AUDITIONS EN RÉUNION PLÉNIÈRE

Mardi 17 décembre 2024 :

- Table ronde avec les organisations professionnelles :

  Pour la CPME : Mme France **CHARRUYER**, membre de la commission numérique, MM. Lionel **VIGNAUD**, directeur des affaires économiques, juridiques et fiscales, Jérôme **NORMAND**, économiste

  Pour le MEDEF : MM. Adrien **DUFOUR**, responsable des affaires publiques, Maxime **FORET,** chargé de mission sénior au sein du pôle Affaires publiques, Mmes Maxence **DEMERLÉ**, directrice du numérique et Mathilde **BRIARD**, chargée de mission économie numérique

- Audition de M. Vincent **STRUBEL**, directeur général de l'Agence nationale de sécurité des systèmes d'information

Jeudi 23 janvier 2025 :

Table ronde avec les experts de la cybersécurité :

Pour l'ACN : MM. Daniel **LE COGUIC**, Président, Yoann **KASSIANIDES**, Délégué général, Mme Elsa **AURIOL**, Responsable des Affaires publiques et M. Farid **LAHLOU**

Pour le Clusif : M. Benjamin **LEROUX**, administrateur

Pour le CyberCercle : MM. Christian **DAVIOT**, Stéphane **MEYNET**, et François **COUPEZ**, senior advisors

Cybertaskforce **:** MM. Sébastien **GARNAULT**, Philippe **LUC**, et Mme Anne Elise **JOLICART**

Lundi 27 janvier 2025 :

Audition de Mme Clara CHAPPAZ, ministre déléguée chargée de l'intelligence artificielle et du numérique

Mardi 4 février 2025 :

Table ronde avec les associations d'élus :

Pour l'association des départements de France et Association des maires de France : M. Michel **SAUVADE**, Vice-Président du conseil Départemental du Puy de Dôme et maire de Marsac-en-Livradois

Pour l'association des régions de France : M. Jérôme **TRÉ-HARDY**, Conseiller régional de Bretagne, Mmes Constance **NEBBULA**, Vice-Présidente de la Région des Pays de la Loire chargée du numérique et Laure **PRÉVOT**, conseillère économie

Pour Intercommunalités de France : Mme Marlène **LE DIEU DE VILLE**, vice-présidente en charge du numérique d'Intercommunalités de France, vice-Présidente déléguée à l'économie numérique, aux systèmes d'information et à la culture de la communauté de communes de Lacq-Orthez, M. Clément **BAYLAC**, conseiller numérique d'Intercommunalités de France et Mme Montaine **BLONSARD**, Responsable des relations avec le Parlement

Pour la Métropole du Grand Paris : M. Geoffroy **BOULARD**, maire du 17e arrondissement, conseiller de Paris, vice-Président de la Métropole du Grand Paris, Mme Justine **TERZI**, chargée de mission Cyber - et M. Eloy **LAFAYE**, chef de projet Innovation numérique

Mardi 11 février 2025 :

- Table ronde avec les autorités de régulation financière

Pour l'Autorité de contrôle prudentiel et de résolution : Mme Véronique **BENSAID-COHEN**, conseillère parlementaire auprès du Gouverneur -Cabinet du Gouverneur Banque de France, MM. Frédéric **HERVO**, Secrétaire général adjoint, Alexandre **GARCIA**, expert en régulation prudentielle bancaire et politique de stabilité financière et M. Gabriel **PREGUIÇA**, chargé de mission

Pour l'Autorité des marchés financiers : MM. Sébastien **RASPILLER**, Secrétaire général et Philippe **SOURLAS**, Secrétaire général adjoint en charge de la Direction de la gestion d'actifs

- Table ronde avec les entreprises de cyberdéfense

Pour Airbus : MM. Michaël **BARTHELLEMY,** Ho Cyber Risk and Assets Management d'Airbus / OCSSI / Autorité d'homologation et Olivier **MASSERET**, Directeur des relations institutionnelles

Pour Orange : MM. Olivier **BONNET DE PAILLERETS,** Executive Vice President Technology & Marketing (Orange Cyberdefense), Patrick **GUYONNEAU,** Directeur de la Sécurité Groupe (Orange) et Laurentino **LAVEZZI,** Directeur des Affaires publiques Groupe

Pour Thales : M. Alexis **CAURETTE**, vice-Président stratégie cybersécurité et Mme Isabelle **CAPUTO,** directrice des relations institutionnelles

II. AUDITITIONS DES RAPPORTEURS

Auditions de M. Michel CANÉVET

Mercredi 11 décembre 2024 :

Direction générale du Trésor : Mmes Camille **SUTTER**, Cheffe du pôle affaires internationales, coordination européenne et enjeux technologique du secteur financier, Isabelle **NARDOT,** adjointe à la Cheffe de Bureau du financement et du développement économique des outre-mer ; MM. Victor **MILLARD**, Adjoint au Chef de Bureau entreprises et intermédiaires d'assurance, David **SABBAN**, Adjoint au Chef de Bureau Services bancaires et moyens de paiement, Florian **SURRE,** Adjoint au Chef de Bureau épargne et marché financier, Thomas **DURANTET**, Adjoint au Conseiller du Directeur général, Arthur **FRAPPEREAU,** Adjoint à la Cheffe du pole affaires internationales, coordination européenne et enjeux technologique du secteur, Sofien **ABDALLAH** : Conseiller parlementaire et relations institutionnelles de la DG Trésor

Jeudi 16 janvier 2025 :

Paris Europlace *:* MM. Olivier **VIGNA**, Délégué général adjoint et Corentin **LANCRENON**, président du groupe de travail Cybersécurité

Fédération bancaire française (FBF) : MM. François **LEFEBVRE**, Directeur général adjoint, Jérôme **RAGUÉNÈS**, Directeur du département Numérique et Moyens de paiement, Jérôme **PARDIGON**, Directeur Relations institutionelles et Olivier **NAUTET**, RSSI de BNP-Paribas

France Assureurs : Mmes Mélodie **LELOUP-VELAY**, Directrice Droit et Conformité, Anne-Marie **PAPEIX**, Responsable RC Médicale, RC Entreprises, Environnement et Cyber et M. Arnaud **GIROS**, Responsable affaires parlementaires

Association des assureurs mutualistes (AAM) : Mme Marie-Ange **GNAHORE** : juriste cyber-sécurité – Groupe AG2R la Mondiale, MM. Xavier **MIGAUD** : RSSI du même groupe, Amadou **DIAWARA** en charge du programme DORA pour le même groupe et Mme Emanuela **MELINTE** , chargée des affaires européennes – AAM

Association française des sociétés financières (ASF) : Mme Solenne **LEPAGE**, Déléguée générale de l'ASF, M. Yves-Marie **LEGRAND**, Délégué général adjoint et Mme Karine **RUMAYOR**, Responsable du service des Études juridiques, comptables, fiscales et prudentielles

Association française des établissements de paiement et de monnaie électronique (AFEPAME) : MM. Michaël **PICCIOLONI**, Président de l'AFEPAME, Pierre **FRANÇON** et Guillaume **PONSARD**

Auditions de M. Patrick CHAIZE

Mercredi 8 janvier 2025 :

- Huawei France – M. Minggang **ZHANG**, directeur général adjoint et Mme Myrian **LAGARDE-FEIGUELMAN**, directrice des affaires institutionnelles.

- Agence nationale des fréquences – M. Gilles **BREGANT**, directeur général et M. Christophe **DIGNE**, directeur général adjoint.

- Numeum – Mme Isabelle **ZABLIT-SCHMITZ**, déléguée générale adjointe ; Mme Marine **GOSSA**, déléguée aux affaires publiques ; Mme Léa **ROUBINET** : chargée de projet cybersécurité.

- Plateforme automobile – M. Mathieu **COULAUD**, secrétaire général, M. Maxime **ANTOINE**, responsable gouvernance et réglementations cybersécurité au sein de la direction de la sécurité de Renault, Mme Stéphanie **GAUTREAU**, de la direction des affaires publiques de Renault et Mme Louise **d'HARCOURT**, responsable des affaires publiques et parlementaires de la PFA.

- Société CISCO France – M. Jean-Charles **GRIVIAUD**, Chief Security Officer et Mme Julie **ROBIN**, responsable des affaires publiques.

Jeudi 9 janvier 2025 :

- Audition commune avec France Industrie (M. Jean-Philippe **THIERRY**, directeur Innovation et industrie du futur) + Fédération des industries électriques, électroniques et de communication (FIEEC) (M. Aridge **KHAYATI**, chargé des affaires publiques) + Fédération des industries mécaniques (FIM) (Mme Roxana **TURCANU**, responsable réglementation technique) ;

- Audition commune avec FedeRez + Fédération des fournisseurs d'accès Internet associatifs (Fédération FDN) – MM. Tom **BARTHE**, Dorian **BOURGEOISAT** et Cédric **HALBER**) ;

- Audition commune des sociétés SERGI TP (M. Antoine **MAGNIER**, président) + P4S (M. Joël **COURTOIS**, président, et M. Yves

DUFAYET, directeur commercial) + SECLAB (M. Xavier **FACELINA**, directeur technique) ;

- Mme Smara **LUNGU**, Directrice Stratégie, Marketing, Communication et Relations institutionnelles chez Docaposte ; M. Matthieu **HENTZIEN**, Directeur de la sécurité des systèmes d'information de Docaposte ; Mme Rebecca **PERES**, Déléguée aux affaires territoriales et parlementaires de La Poste.

Vendredi 10 janvier 2025 :

- Société HEXATRUST (Mme Dorothée **DECROP**, déléguée générale) + OVH cloud (Mme Blandine **EGGRICKX**, responsable des affaires publiques, M. Julien **LEVRARD**, RSSI)

Lundi 13 janvier 2025 :

Club des experts de la sécurité de l'information et du numérique (CESIN) – M. Alain **BOUILLE**, délégué général

Vendredi 17 janvier 2025 :

Fédération française des télécommunications (FFT) : MM. Patrick **GUYONNEAU**, président de la commission de la sécurité de la FFT et directeur de la sécurité du groupe Orange, Olivier **RIFFARD**, directeur général adjoint de la FFT et Alexandre **GALDIN**, directeur délégué aux études économiques, à l'environnement et à la sécurité de la FFT.

Groupe Orange : M. Franck **LAURENT**, juriste et Mme Pauline **CAYATTE**, direction des affaires publiques chez Orange.

Groupe Bouygues Télécoms : M. Henri **FAVREAU**, expert cybersécurité chez Bouygues Télécom.

Groupe Altice-SFR : MM. Matthieu **HENNEBO**, directeur Cybersécurité Altice France et Éric **GYSELINCK**, expert cybersécurité chez Altice France.

Groupe Iliad-Free : Mmes Julie **GOMMES**, directrice Cybersécurité et

Ombeline **BARTIN**, directrice des affaires publiques.

Auditions de M. Hugues SAURY

Mercredi 11 décembre 2024 :

Secrétariat général de la défense et de la sécurité nationale (SGDSN) : MM. Arthur **DANIN**, Gwénael **JEZEQUEL** et Alexandre **NÈGRE**

Mercredi 15 janvier 2025 :

Direction générale de l'armement : Ingénieur général Pascal **FINTZ**, chef de service de la sécurité de défense des systèmes d'information et M. Mathieu **JACQUART,** chef du bureau de la protection et de la réglementation

Mardi 28 janvier 2025 :

Groupement des Industries Françaises Aéronautiques et Spatiales (GIFAS) : MM. Michaël Henri Paul **BARTHELLEMY,** Responsables des risques et vulnérabilités cyber pour le groupe Airbus, Christophe **Floch,** Responsable de la Sécurité des Systèmes d'Information groupe Dassault Aviation et Jérôme **JEAN,** Directeur des Affaires publiques

Groupement des Industries Françaises de Défense et de Sécurité Terrestres et Aéroterrestres (GICAT) : MM. Jean-Jacques **Pellerin**, Consultant cyber et Eric **Marini**, Directeur des Systèmes d'Information du groupe Etienne Lacroix,

Groupement des Industries de Construction et Activités Navales (GICAN) : Mme Claudie **BENOIT**, Responsable affaires techniques, environnement et sécurité,

Direction de la protection des installations, moyens et activités de la Défense : MM. Nicolas **Leverrier**, général de division aérienne, Mme Sophie **Griffe**, fonctionnaire de sécurité des systèmes d'information du ministère des Armées et Colonel Cyrille **Caron**, fonctionnaire sécurité - défense du ministère des Armées

Fédération professionnelle des entreprises de services pour l'énergie et l'environnement (FEDENE) : M. Pascal **GUILLAUME**, Président, Mme Marion **LETTRY**, déléguée générale et M. Bertrand **NACHBAUR**, Directeur des Systèmes d'Information et du Numérique de Dalkia

Mardi 11 février 2025 :

F2PE Les entreprises de l'eau : MM. Jean-Paul **COURCIER**, Coordinateur National Gestion d'alerte et de crise, Correspondant Sûreté Eau France - Veolia, Matthieu **BERTIN**, Responsable de la sécurité des systèmes d'information - Veolia, Antoine **ANCEL** Directeur Cyber Sécurité Opérationnelle - RSSI – Suez Christophe **MAÏSSA**, Référent national sûreté, Direction technique – Suez,

Mmes Aurélie **COLAS**, Déléguée générale – FP2E et Claire **BALDACCI**, Conseillère affaires publiques – FP2E

Enedis : M. Vincent **DUFOUR**, directeur des affaires publiques et Mme Jasmine **JOURDAIN,** chargée d'affaires parlementaires

LISTE DES CONTRIBUTIONS ÉCRITES

Alliance pour la Confiance Numérique (ACN)

Association française des entreprises privées (AFEP)

Cabinet de conseil IDATE

Confédération des petites et moyennes entreprises (CPME)

Cyber Cercle

Cyber Task Force

Fédération des Industries Electriques, Electroniques et de Communication (FIEEC)

Intercommunalités de France

Mouvement des entreprises de France (Medef)

Union des entreprises de proximité (U2P)

Syndicat national des entreprises fabricantes de dispositifs médicaux (Snitem)

Société Kaspersky France

Société Sesame IT

LISTE DES DÉPLACEMENTS

DÉPLACEMENT D'UNE DÉLÉGATION À BRUXELLES, LE MARDI 10 DÉCEMBRE 2024

Direction générale CONNECT de la Commission européenne

- Entretien avec **Mme Christiane KIRKETERP de VIRON**, Directrice chargée de la cybersécurité

Direction générale de la stabilité financière, des services financiers et de l'union des marchés des capitaux et direction générale chargée des affaires intérieures de la Commission européenne

- Entretien avec **M. Boris AUGUSTINOV** de la DG FISMA et **Mme Heike BUSS** de la DG HOME

Banque nationale de Belgique :

- Entretien avec **M. Thomas Plomteux,** Head of IT Prudential Supervision, **Mme Liesbeth Denturck,** conseillère juridique**, M. Geoffroy Delrée,** directeur adjoint gestion des affaires publiques, institutionnelles et projets stratégiques, et **M. Antoine Greindl,** juriste FSMA

Centre belge pour la cybersécurité (CCB) :

- Entretien avec **M. Miguel DE BRUYCKER,** Directeur, **Mme Phédra CLOUNER,** Directrice-adjointe, **M. Pieter BYTTEBIER,** Responsable relations internationales, **M. Valéry VANDER GEETEN,** Responsable juridique et coordinateur de la transposition NIS2

LA LOI EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, visualiser les apports de chaque assemblée, comprendre les impacts sur le droit en vigueur, le tableau synoptique de la loi en construction est disponible sur le site du Sénat à l'adresse suivante :

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