N° 1779

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

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

RAPPORT

FAIT

AU NOM DE LA COMMISSION SPÉCIALE [1] CHARGÉE D'EXAMINER LE PROJET DE LOI, adopté par le sénat, après engagement de la procédure accélérée, *relatif à la* **résilience** *des* **infrastructures critiques** *et au* **renforcement** *de la* **cybersécurité** (n° 1112),

PAR M. ÉRIC BOTHOREL
Rapporteur général,

ET

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

TOME I :
SYNTHÈSE, COMMENTAIRES DES ARTICLES, PERSONNES AUDITIONNÉES

Voir les numéros :

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

Assemblée nationale : **1112**.

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

La commission spéciale est composée de :

M. Philippe Latombe, *président* ;

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

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

M. Éric Bothorel, *rapporteur général* ;

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

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

SOMMAIRE

___

Pages

AVANT-PROPOS DU RAPPORTEUR GÉNÉRAL

Le 14 décembre 2022, le Parlement européen et le Conseil ont adopté trois directives concernant :

– la résilience des entités critiques (REC) [(1)] ;

– les mesures destinées à assurer un niveau élevé commun de cybersécurité (NIS 2) [(2)] ;

– la résilience opérationnelle numérique du secteur financier (DORA) [(3)].

Les États membres avaient respectivement jusqu'au 17 octobre 2024 pour transposer dans leur droit interne les directives REC et NIS 2 et jusqu'au 17 janvier 2025 pour la directive DORA.

Dans notre pays, cette transposition a pris du temps en raison de la dissolution de l'Assemblée nationale, de la censure du gouvernement de M. Michel Barnier et, en conséquence, de l'encombrement du calendrier législatif.

Les 9 et 10 septembre 2025, la commission spéciale a enfin pu examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Il avait été adopté par le Sénat en première lecture le 12 mars.

Après avoir discuté de 472 amendements, elle en a adopté 244, présentés par les différents groupes représentés en son sein.

Dès le début de ses travaux, le rapporteur général s'est fixé pour ligne de conduite d'éviter tant la sur-transposition que la sous-transposition des trois directives faisant l'objet du projet de loi. D'autant plus que la démission du gouvernement de M. François Bayrou n'autorisait guère les membres de la commission spéciale à s'émanciper du cadre posé par ces actes européens. Le rapporteur général a ainsi veillé, par ses avis, à ce que la discussion obéisse à ces principes.

Il salue par ailleurs la qualité du travail des rapporteurs de chaque titre du projet de loi – Mme Catherine Hervieu (titre Ier), Mme Anne Le Hénanff (titre II) et M. Mickaël Bouloux (titre III) – et n'a pas manqué de reprendre à son compte et de soutenir un nombre important de leurs amendements.

Les travaux de la commission spéciale sont intervenus alors que l'actualité ne cesse de faire état de cyberattaques. Ont ainsi été victimes, au cours des derniers mois, le centre communal d'action sociale de Poitiers, le logiciel Kairos de France Travail, le constructeur

---

(1) Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil.

(2) 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.

(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.

automobile Jaguar Land Rover, le Muséum national d'histoire naturelle, l'entreprise Naval Group, les services sociaux du conseil départemental de l'Aude, le groupe Auchan, les opérateurs de télécommunication Orange et Bouygues. La diversité des organismes touchés témoigne de la diffusion de la menace cyber dans notre pays.

« *Ils ne mouraient pas tous, mais tous étaient frappés* », pourrait-on dire en paraphrasant Jean de La Fontaine dans *Les Animaux malades de la peste.*

Le rapporteur général tient à rappeler que la menace cyber peut affecter toutes et tous. Le présent projet de loi doit œuvrer à la résilience de tous les maillons de la chaîne. Il répond à la nécessité de renforcer la capacité de notre économie et de notre société à surmonter ces attaques. Comme le soulignait le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en audition, « *cette menace, actuellement opportuniste, pourrait un jour, s'avérer coordonnée avec des menaces étatiques dans un contexte géopolitique plus large* ».

Face à cette situation, l'Union européenne a élaboré la directive NIS 2 grâce à l'impulsion de la France. Elle complète un cadre législatif européen préexistant tout en s'inscrivant dans une nouvelle logique. La directive représente aussi un changement d'échelle radical s'agissant du nombre d'entités régulées.

Le rapporteur général rappelle également que la résilience n'est pas un sujet nouveau. Dès octobre 2015, l'État est parti du constat, au travers de sa stratégie nationale pour la sécurité du numérique, que s'il était plutôt en mesure de protéger ses propres infrastructures ou les infrastructures vitales du pays, il se devait d'apporter une réponse structurée aux autres composantes de la société, souvent désarmées face à une cybercriminalité en plein essor. C'est de cette volonté qu'est né le groupement d'intérêt public (GIP) d'action contre la cyber-malveillance (ACYMA) en mars 2017 qui pilote actuellement le site internet cybermalveillance.gouv.fr dédié à la sensibilisation, à la prévention et à l'assistance aux victimes, qu'il s'agisse de particuliers, d'entreprises ou de collectivités territoriales. Dans cet élan, le renforcement des moyens de l'ANSSI doit se poursuivre, notamment au regard des nouvelles compétences que ce projet de loi lui confère.

La sécurisation et la régulation de l'espace numérique progressent mais les attaquants avancent toujours plus vite. Les acteurs du numérique attendent ce projet de loi et en espèrent des dispositions claires et précises. Il doit aussi être l'occasion de sensibiliser nos compatriotes à la cybersécurité.

Ainsi, le rapporteur général ne peut que se réjouir que la commission spéciale ait adopté à l'unanimité ce projet de loi, modifié par les apports de son président, de ses rapporteurs thématiques, de ses différents membres ainsi que des siens. Le présent rapport fait état de l'ensemble de ses travaux.

*

* *

SYNTHÈSE

I. LES DISPOSITIONS DU PROJET DE LOI INITIAL

A. TITRE IER : LA TRANSPOSITION DE LA DIRECTIVE REC CONDUIT À UN RENFORCEMENT DU DISPOSITIF DE SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

L'article 1er du projet de loi transpose en droit national la directive du 14 décembre 2022, dite REC [(1)], sur la résilience des entités critiques, en modifiant les articles L. 1332-1 et suivants du code de la défense. Les obligations prévues par la directive sont inspirées de celles prévues en France, depuis 2006, par le dispositif de sécurité des activités d'importance vitale (SAIV). Ainsi, la transposition de la directive se traduit par une actualisation du dispositif de SAIV, afin de renforcer le cadre existant qui a montré son efficacité.

Le dispositif de SAIV vise à garantir la protection des points d'importance vitale (PIV), désignés par l'État, essentiels au potentiel économique et militaire de la nation. Prévu aux articles L. 1332-1 à L. 1332-7 du code de la défense, le dispositif s'applique aux opérateurs d'importance vitale (OIV), publics et privés, qui exploitent les établissements et ouvrages dont l'indisponibilité menacerait la continuité de la vie de la nation ou qui pourraient constituer un danger grave pour la population. Le dispositif actuel concerne environ 300 OIV et 1 500 PIV, dont la liste est classifiée. Les OIV concernent des entreprises, publiques et privées, et des administrations, qui gèrent des sites sensibles : usines, centrales nucléaires, hôpitaux, bases militaires etc.

Le dispositif est fondé sur une planification assurée par l'État et les OIV pour garantir la sécurité de leurs sites sensibles et la continuité de leur activité. L'opérateur doit établir un plan de sécurité opérateur (PSO) et un plan particulier de protection (PPP) pour chaque PIV.

Le premier ministre fixe la liste des secteurs éligibles au dispositif et approuve les directives nationales de sécurité (DNS) qui décrivent les besoins de sécurité pour chaque secteur. Le secrétariat général de la défense et de la sécurité nationale (SGDSN) coordonne le dispositif au niveau national, décliné au niveau territorial par les préfectures et animé pour chaque secteur d'activité par les ministères coordonnateurs dans leur champ de compétences, au travers du service du haut fonctionnaire de défense et de sécurité.

---

(1) Directive 2022/2557 du Parlement et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/C du Conseil.

La directive REC, négociée sous présidence française de l'Union européenne, fixe des règles minimales harmonisées pour garantir la fourniture, dans le marché intérieur, des services considérés comme essentiels au maintien de fonctions sociétales ou économiques vitales. Elle remplace la directive du 8 décembre 2008 (1), qui se limitait à recenser les infrastructures critiques dans les secteurs de l'énergie et des transports et à prévoir leur protection physique par les États membres. Une évaluation menée par la Commission européenne en 2019 a souligné la nécessité de mettre à jour le dispositif, volonté accrue par la pandémie de Covid de 2020, pour faire face à des nouveaux enjeux : dépendance énergétique, cybersécurité, changement climatique, souveraineté numérique, sécurité économique.

La directive REC s'inscrit dans une politique de résilience globale, puisque les entités seront également soumises aux obligations de cybersécurité prévues par la directive du 14 décembre 2022, dite NIS 2 (2), et transposées dans le titre II du projet de loi. Elle s'applique aux entités critiques, c'est-à-dire à toute entité publique ou privée désignée par un État membre et opérant dans un secteur stratégique. La résilience est entendue comme la capacité d'une entité à prévenir tout incident, à s'en protéger, y réagir, l'atténuer, l'absorber et s'en rétablir. En vertu de la directive, les États doivent notamment développer une stratégie nationale de résilience, recenser les entités critiques et déterminer un régime de sanctions. Les entités doivent, de leur côté, procéder à une évaluation des risques et mettre en œuvre des mesures de sécurité, détaillées au sein d'un plan.

Les principales modifications du dispositif de SAIV à la suite de la transposition de la directive REC sont les suivantes :

– le plan de résilience opérateur se substitue au plan de sécurité opérateur, avec une notion de continuité de l'activité et d'analyse des risques et des dépendances ;

– une astreinte pourra être imposée aux opérateurs, publics et privés, qui refusent de se mettre en conformité avec leurs obligations ;

– le champ des enquêtes administratives pour contrôler l'accès aux sites est étendu aux accès à distance et l'avis de l'autorité administratif passe de simple à conforme ;

– les opérateurs devront signaler les incidents à l'autorité administrative ;

---

(1) Directive 2008/114/CE concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

(2) 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) (Texte présentant de l'intérêt pour l'EEE).

– la notion d'entité critique d'importance européenne particulière est introduite en droit national, c'est-à-dire les opérateurs qui réalisent des activités similaires dans au moins six États membres de l'Union ;

– le régime de sanctions pénales, actuellement prévu par le dispositif, est remplacé par un régime de sanctions administratives, et une commission des sanctions est instituée pour réprimer les manquements des opérateurs.

Ces nouvelles obligations conduiront à un surcroît d'activité modéré pour les opérateurs, déjà pour la plupart sensibilisés à la prévention des risques et la continuité de leur activité. Néanmoins, le délai réduit de réalisation des nouveaux plans, en particulier celui de dix mois prévu pour le plan de résilience opérateur, pourrait causer quelques difficultés aux opérateurs et à l'autorité administrative pour faire la transition vers le dispositif actualisé.

En outre, la transposition de la directive conduit à l'élargissement des secteurs couverts par le dispositif à trois nouveaux secteurs, à savoir l'assainissement de l'eau, les réseaux de chaleur et de froid et l'hydrogène. Le nombre d'opérateurs d'importance vitale ne devrait pas évoluer de manière significative.

L'article 2 procède à des actualisations législatives pour tirer les conséquences du dispositif introduit à l'article 1er du présent projet de loi. Il actualise le code de la défense, le code pénal, le code des postes et des communications électroniques, le code de la santé publique, le code la sécurité intérieure et la loi n° 2006-961 du 1er août 2006 relative aux droits d'auteur et aux droits voisins.

L'article 3 prévoit les modalités d'application du dispositif introduit à l'article 1er en outre-mer. Le dispositif s'appliquera sur l'ensemble du territoire national, qu'il s'agisse des collectivités d'outre-mer régies par le principe d'identité législative ou de spécialité législative.

L'article 4 prévoit les modalités d'entrée en vigueur des dispositions prévues au titre Ier. Le texte initial ne prévoyant pas de date d'entrée en vigueur, il serait entré en vigueur au lendemain de la publication du projet de loi au *Journal officiel.*

B. TITRE II : LA TRANSPOSITION DE LA DIRECTIVE NIS 2 A POUR OBJECTIF DE RENFORCER SIGNIFICATIVEMENT LA CYBERSÉCURITÉ DE LA NATION

L'article 5 désigne l'ANSSI comme cheffe de file, à l'échelle nationale, pour la mise en œuvre de la politique du gouvernement en matière de sécurité des systèmes d'information.

L'article 6 définit les principales notions nécessaires à la mise en œuvre du dispositif national de cybersécurité tel qu'imposé par la directive NIS 2.

L'article 7 renvoie à un décret en Conseil d'État l'établissement de la liste des secteurs d'activité critiques et hautement critiques pour le fonctionnement de l'économie et de la société.

L'article 8 liste les 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 la directive NIS 2.

L'article 9 liste les entités considérées comme « importantes » du point de vue de la sécurité des systèmes d'information et qui, à ce titre, se verront appliquer les dispositions prévues par la directive NIS 2.

L'article 10 donne la faculté au premier ministre de désigner par arrêté comme entité « essentielle » ou « importante » une entité exerçant une activité relevant d'un secteur d'activité hautement critique ou critique en fonction de critères prévus à cet effet.

L'article 11 définit les règles de compétences des États membres pour l'application des dispositions de la directive selon des critères territoriaux.

L'article 12 prévoit que l'ANSSI établit et met à jour la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement sur la base des informations communiquées par ces entités et ces bureaux d'enregistrement.

L'article 13 prévoit 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.

L'article 14 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'information 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.

L'article 15 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.

L'article 16 confère au premier ministre le pouvoir de rajouter des obligations supplémentaires en matière de cybersécurité aux OIV ainsi qu'aux administrations les plus sensibles.

L'article 17 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. Il prévoit également que l'ANSSI peut exiger qu'une entité ayant fait l'objet d'un incident de cybersécurité en informe le public, voire en informer directement le public.

L'article 18 détermine les offices d'enregistrement et les bureaux d'enregistrement auxquels s'appliquent les dispositions de la section 3

« Enregistrement des noms de domaine » du projet de loi selon les critères territoriaux fixés à l'article 11.

L'article 19 oblige les offices et les bureaux d'enregistrement des noms de domaine à 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.

L'article 20 fixe la durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaines, en prévoyant qu'ils doivent conserver les données relatives à chaque nom de domaine dans leur base de données tant que le nom de domaine est utilisé.

L'article 21 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.

L'article 22 prévoit que les offices et les bureaux d'enregistrement devront mettre en place des procédures permettant à l'ANSSI et à l'autorité judiciaire d'accéder aux données collectées relatives aux noms de domaine, à leur demande, dans un délai maximal de 72 heures.

L'article 23 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.

L'article 24 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.

L'article 25 autorise 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.

L'article 26 permet 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.

L'article 27 précise 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.

L'article 28 oblige la personne contrôlée par l'ANSSI à coopérer avec elle et instaure une amende administrative en cas d'obstacle au contrôle.

L'article 29 prévoit les formes que pourraient revêtir les contrôles de l'ANSSI et en fait supporter le coût par la personne contrôlée.

L'article 30 renvoie 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.

L'article 31 permet à l'ANSSI d'ouvrir une procédure à l'encontre de la personne contrôlée au vu des résultats du contrôle.

L'article 32 détermine la manière dont pourrait se poursuivre une procédure ouverte par l'ANSSI à l'encontre de la personne contrôlée, en particulier les mesures d'exécution pouvant être mises en œuvre.

L'article 33 prévoit la saisine par l'ANSSI de la commission des sanctions en cas d'inexécution d'une mesure d'exécution.

L'article 34 renvoie 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.

L'article 35 prévoit que la commission des sanctions, placée auprès du premier ministre et créée par l'article 1er du projet de loi, est compétente pour statuer sur l'application des dispositions du chapitre II « De la cyber-résilience » et du chapitre III « De la supervision » du présent projet de loi.

L'article 36 précise la composition de la commission des sanctions.

L'article 37 transpose les différentes sanctions administratives prévues par la directive NIS 2 en cas de méconnaissance des obligations imposées aux entités régulées.

L'article 38 allège le contrôle des moyens et prestations de cryptologie en passant d'un dispositif d'autorisation à un régime de déclaration préalable en matière d'exportation.

L'article 39 abroge la directive NIS 1 et procède à une simplification du cadre réglementaire pour tenir compte de la transposition de la directive NIS 2.

L'article 40 étend l'application du titre II du projet de loi aux collectivités d'outre-mer régies par le régime de spécialité législative.

L'article 41 renforce les sanctions pénales pour améliorer la lutte contre les brouillages.

L'article 42 renforce les conditions d'accès à une assignation de fréquences déposée par la France auprès de l'Union internationale des télécommunications (UIT).

C. TITRE III : LA TRANSPOSITION DE LA DIRECTIVE DORA ENTEND RENFORCER LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DES ENTITÉS FINANCIÈRES

Le chapitre Ier modifie le code monétaire et financier en répercussion des changements opérés par la directive sur la résilience opérationnelle numérique du secteur financier (DORA) dans plusieurs directives sectorielles déjà transposées dans le droit interne.

L'article 43 remplace le terme de « *technologie de l'information* » par « *technologie de l'information et de la communication* » (TIC) dans la définition des services de paiement.

L'article 44 introduit une référence à la gestion du risque lié aux TIC et aux tests de résilience opérationnelle numérique, prévus par le règlement 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA), dans les exigences opérationnelles des gestionnaires de plates-formes de négociation.

L'article 45 introduit une référence à la gestion du risque lié aux TIC, prévue par le règlement DORA, dans les obligations des sociétés qui gèrent un marché réglementé.

L'article 46 met en cohérence les exigences prudentielles des prestataires de services bancaires avec la prise en compte renforcée du risque lié aux TIC par le règlement DORA.

L'article 47 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans le dispositif de gouvernance des prestataires de services bancaires.

L'article 48 impose aux prestataires de services de paiement de respecter le cadre de gestion du risque lié aux TIC établi par le règlement DORA dans les procédures de contrôle des risques opérationnels de sécurité.

L'article 49 prévoit de réserver les obligations de déclaration des incidents majeurs, actuellement en vigueur pour l'ensemble des prestataires de services de paiement, à la Banque de France, au Trésor public et à la Caisse des dépôts et consignations du fait de nouvelles règles issues du règlement DORA en la matière.

L'article 50 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les dispositifs de contrôle et de sauvegarde de leurs systèmes informatiques des entreprises d'investissement et des entreprises de crédit.

L'article 51 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les règles d'organisation des prestataires de services d'investissement.

L'article 52 introduit une référence à la gestion du risque lié aux TIC, à la réponse aux incidents, au rétablissement des services et à la conduite de tests de résilience opérationnelle numérique dans le dispositif de prévention et de contrôle des incidents liés à la négociation algorithmique des entreprises d'investissement et des entreprises de crédit.

L'article 53 *(supprimé)* incluait les prestataires tiers de services fondés sur les TIC dans la liste des organismes susceptibles de devoir communiquer tous documents ou renseignements à l'Autorité de contrôle prudentiel et de résolution (ACPR).

L'article 54 introduit une référence à la résilience opérationnelle numérique ainsi qu'aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les plans de résolution établis par le collège de résolution de l'ACPR.

L'article 55 étend à la Banque de France et à l'ACPR l'habilitation à échanger des informations relatives à la sécurité des systèmes d'information avec l'Autorité des marchés financiers (AMF) et l'ANSSI.

L'article 56 rend applicable en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna les dispositions du chapitre Ier du titre III.

Le chapitre II modifie le code des assurances en répercussion des changements opérés par la directive DORA dans la directive « solvabilité II » déjà transposée dans le droit interne.

L'article 57 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les règles prudentielles des entreprises d'assurance et de réassurance.

L'article 58 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les règles prudentielles des groupes du secteur de l'assurance.

Le chapitre III modifie le code de la mutualité en répercussion des changements opérés par la directive DORA dans la directive « solvabilité II ».

L'article 59 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les règles prudentielles des mutuelles et de leurs unions.

L'article 60 supprime une redondance rédactionnelle du fait de l'application des articles 57 à 59.

Le chapitre IV modifie le code de la sécurité sociale en répercussion des changements opérés par la directive DORA dans la directive « solvabilité II ».

L'article 61 introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA dans les règles prudentielles des institutions de prévoyance et de leurs unions.

Le chapitre V comporte les dispositions finales pour l'application du titre III.

L'article 62 détermine les modalités d'entrée en vigueur des dispositions du titre III.

II. LES MODIFICATIONS INTRODUITES PAR LE SÉNAT

A. TITRE IER

À **l'article 1er**, les principales modifications apportées par le Sénat sont les suivantes :

– les notions d'incident et de résilience ont été définies ;

– l'astreinte journalière a été précisée comme s'appliquant 24 heures après la mise en demeure ;

– la notification d'incidents à l'autorité administrative devra intervenir au plus tard 24 heures après la notification et un décret en Conseil d'État précisera les conditions de mise en œuvre de l'obligation de notification ;

– les conditions de saisine de la Commission européenne pour effectuer une mission de conseil ont été précisées ;

– les personnalités qualifiées membres de la commission des sanctions seront nommées par le premier ministre, le président de l'Assemblée nationale et le président du Sénat, et pas seulement par le premier ministre.

L**'article 4** a été modifié pour préciser que le titre Ier entrera en vigueur à une date fixée par décret en Conseil d'État, au plus tard un an après la promulgation de la présente loi, pour laisser le temps aux opérateurs de se conformer aux nouvelles obligations, en attendant la publication des actes d'application.

B. TITRE II

Les principales modifications apportées par le Sénat sont les suivantes :

– désignation de l'ANSSI comme autorité nationale compétente et précision du champ des missions de l'ANSSI (accompagnement et soutien au développement de la filière cybersécurité) (**article 5**) ;

– introduction de l'élaboration par le premier ministre d'une stratégie nationale en matière de cybersécurité (**article 5 *bis***) ;

– introduction des définitions des notions d'incident et de vulnérabilité (**article 6**) ;

– introduction de la liste des secteurs hautement critiques et critiques tels qu'ils figurent en annexe de la directive NIS 2 (**article 7**) ;

– exclusion des communautés d'agglomération ne comprenant pas au moins une commune d'une population supérieure à 30 000 habitants de la liste des entités essentielles (**article 8**) et importantes (**article 9**) ;

– mise à jour de la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement concernés par le titre II du projet de loi *a minima* tous les deux ans (**article 12**) ;

– transmission des informations à l'ANSSI par les entités essentielles et importantes et les bureaux d'enregistrement dans le respect des modalités de chiffrement de bout en bout ainsi que de la protection des données recueillies de l'effet des lois extraterritoriales (**article 12**) ;

– adaptation du référentiel d'exigences techniques aux spécificités des acteurs mentionnés au premier alinéa de l'article 14 du projet de loi, en fonction de leur degré d'exposition au risque, de leur taille, de la probabilité de survenance d'un incident et de leur gravité (**article 14**) ;

– prise en compte des modalités de concertation des représentants des entités concernées et des associations d'élus dans l'élaboration du référentiel d'exigences techniques (**article 14**) ;

– création d'un mécanisme de reconnaissance mutuelle entre les États membres de l'Union européenne et vers d'autres types de référentiels, de sorte qu'une entité qui aurait vu certifiée sa conformité à un référentiel dont le niveau équivalent de sécurité a été validé par l'ANSSI puisse s'en prévaloir lors d'un contrôle (**article 15**) ;

– possibilité de vérifier la conformité au référentiel d'exigences techniques *via* un label de confiance approuvé par l'ANSSI (**article 15**) ;

– introduction d'un article additionnel empêchant d'imposer aux fournisseurs de services de chiffrement l'intégration de dispositifs techniques visant à affaiblir la sécurité des systèmes d'information et des communications électroniques (**article 16 *bis***) ;

– intégration de critères pour considérer qu'un incident est important au sens de la directive et précisions quant à la nature des incidents importants devant être notifiés sans retard injustifié (**article 17**) ;

– introduction de délais de notification aux CERT nationaux des incidents informatiques (**article 17**) ;

– obligation pour les CERT de fournir, sans retard injustifié, une réponse à l'entité émettrice d'une notification alertant d'une cyberattaque (**article 17**) ;

– suppression de la notion d'incident « critique » pour se limiter à la seule notion d'incident « important » prévue dans la directive (**article 17**) ;

– extension du délai de conservation des données par les bureaux d'enregistrement à la durée d'utilisation du nom de domaine et jusqu'à l'expiration d'un délai d'un an à compter de la cessation de l'utilisation de ce nom de domaine (**article 20**) ;

– encadrement de la communication d'informations aux agents habilités par l'autorité judiciaire pour les besoins des procédures pénales et de la sécurité des systèmes d'information (**article 23**) ;

– modification rédactionnelle des dispositions sur le coffre-fort numérique (**article 26 A**) ;

– suppression de la référence aux infractions pouvant être commises par les personnes contrôlées par l'ANSSI, clarification du rôle des agents et personnels des organismes indépendants en matière de recherche des manquements, possibilité pour les agents et personnels habilités par l'ANSSI de concourir à la recherche des manquements (**article 26**) ;

– absence de prise en charge financière par les entités contrôlées du coût du contrôle en cas d'absence de manquement aux obligations prévues par le projet de loi (**article 29**) ;

– introduction des dispositions de l'article 32 du projet de loi dans l'article 31, possibilité pour l'ANSSI de rendre publique la mesure d'exécution adoptée et d'enjoindre à la personne contrôlée de rendre public son manquement, ouverture d'une procédure à l'encontre de l'entité contrôlée lorsque le contrôle révèle des éléments ou des faits éveillant une suspicion de manquement (**articles 31** et **32**) ;

– exclusion des 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 (**article 33**) ;

– saisine de la commission des sanctions par l'ANSSI, nomination par les présidents des deux assemblées de deux des trois personnalités qualifiées membres de la commission des sanctions, limitation de la possibilité de nommer des personnalités qualifiées aux personnes qui n'ont pas exercé, au cours des trois années précédant leur nomination, une activité ni au sein d'une entité essentielle ou importante , ni au sein de l'ANSSI (**article 36**) ;

– restriction de la faculté pour la commission des sanctions d'interdire à toute personne physique exerçant les fonctions de dirigeant dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité, possibilité pour la

commission des sanctions d'exiger que l'entité qui s'est rendue coupable d'un manquement communique au public le manquement constaté, voire que la commission des sanctions rende elle-même public le manquement, nécessité pour la commission des sanctions de prendre en compte les circonstances et la gravité du manquement (**article 37**) ;

– clarification de l'applicabilité en Nouvelle-Calédonie et en Polynésie française des modifications prévues à l'article 39 du projet de loi (**article 40**).

C. TITRE III

Au **chapitre Ier**, les principales modifications apportées par le Sénat sont les suivantes :

– désignation de la Banque de France et de l'ACPR comme seules destinataires des déclarations d'incidents majeurs liés aux TIC et des notifications volontaires de cybermenaces de la part des entités financières qui relèvent de leur compétence, en application de l'article 19 du règlement DORA et dans un but de simplification administrative pour les entreprises (**article 43 A**) ;

– désignation également de l'AMF comme seule destinataire des déclarations d'incidents majeurs liés aux TIC et des notifications volontaires de cybermenaces de la part des entités financières qui relèvent de sa compétence (**article 45 *bis***) ;

– réécriture de **l'article 49** dans un souci de simplification afin, d'une part, de faire de l'ACPR l'unique destinataire des déclarations d'incidents qu'elle doit ensuite transmettre à la Banque de France et, d'autre part, de prévoir expressément que les obligations déclaratives auxquelles sont soumises les entités financières fournissant des services de paiement relèvent du règlement DORA ;

– extension des dispositions du règlement DORA aux succursales d'entreprises d'investissement de pays tiers afin de ne pas créer une rupture de l'égalité avec les autres prestataires de services d'investissement en France (**article 49 *bis***) ;

– suppression de l'**article 53** car la rédaction actuelle de l'article L. 612-24 du code monétaire et financier régissant la transmission des documents et informations devant être périodiquement remis à l'ACPR inclut déjà l'ensemble des tiers auprès desquels les personnes assujetties à cette autorité ont externalisé des fonctions ou activités opérationnelles.

Au **chapitre II**, les sénateurs ont ajouté l'**article 58 *bis*** visant à confier la charge de la preuve à l'assureur en cas de cyberattaque afin que les pertes et dommages que ces sinistres sont susceptibles d'occasionner soient mieux indemnisés.

Au sein des dispositions finales du **chapitre V**, le Sénat a expressément exclu du champ de la directive NIS 2 les entités financières auxquelles s'appliquent le règlement et la directive DORA en ce qui concerne les mesures de gestion des

risques en matière de cybersécurité ou de notification d'incidents importants (**article 62 A**) afin d'éviter tout risque de double assujettissement.

À l'**article 62**, les sénateurs ont modifié la date d'entrée en vigueur des dispositions du titre III :

– au lendemain de la promulgation de la loi de manière générale, compte tenu du retard pris dans l'examen du texte ;

– au 1er janvier 2030 pour l'application des exigences prudentielles propres aux prestataires de services bancaires à l'ensemble des sociétés de financement, sans référence à leur taille, en raison du fait qu'elles ne sont pas expressément visées par la directive DORA et pour tenir compte de leurs spécificités par comparaison aux autres prestataires de services bancaires que sont les établissements de crédit.

Le Sénat a également posé un principe de proportionnalité pour l'application du règlement DORA aux sociétés de financement de petite taille et non complexes.

III. LES MODIFICATIONS APPORTÉES PAR LA COMMISSION SPÉCIALE

A. TITRE IER

À **l'article 1er**, les principales modifications apportées par la commission sont les suivantes :

– clarification entre la notion d'infrastructure critique utilisée en droit européen et celle de point d'importance vitale utilisée en droit national (alinéa 9) ;

– extension de l'analyse des dépendances aux sous-traitants, selon un délai fixé par voie réglementaire, et aux vulnérabilités envers les fournisseurs de solutions logicielles et matérielles propriétaires (alinéa 32) ;

– distinction dans le plan de résilience entre les dispositifs et les dispositions de résilience (alinéa 35) ;

– ajout de l'avis de la Commission nationale de l'informatique et des libertés (CNIL) sur le décret en Conseil d'État précisant les modalités de l'avis de l'autorité administrative sur une autorisation d'accès à un point d'importance vitale (alinéa 40) ;

– mise en cohérence des obligations imposées aux OIV avec celles prévues par la directive NIS 2 (alinéa 60) ;

– nomination des personnalités qualifiées de la commission des sanctions par le premier ministre, plutôt que par le premier ministre, le président de l'Assemblée nationale et le président du Sénat (alinéa 83) ;

– inscription dans le code de la défense de la procédure contradictoire devant la commission des sanctions (alinéa 87) ;

– mandat non renouvelable des membres, hors personnalités qualifiées, de la commission des sanctions (alinéa 90).

B. TITRE II

Les modifications suivantes ont été apportées aux articles du titre II :

– inscription dans les missions de l'ANSSI de la promotion de la cyberprotection, de la cyberhygiène et de l'éducation aux bonnes pratiques numériques (**article 5**) ;

– inscription dans les plans communaux de sauvegarde du risque d'incident informatique ayant un impact important sur la fourniture des services à la population (ajout d'un **article 5 *bis* A**) ;

– intégration dans la stratégie nationale de cybersécurité de l'autonomie stratégique, de mesures pour améliorer le niveau de sensibilisation face au risque cyber, des modalités de soutien financier aux collectivités territoriales, de la création d'un fonds de soutien destiné à accompagner certaines collectivités territoriales et leurs établissements publics, d'une stratégie d'aménagement du territoire pour renforcer la cyber-résilience des territoires, du renforcement de l'offre de formation publique dans les domaines de la cybersécurité et de la cyberdéfense et d'orientations pour promouvoir le recours aux logiciels libres (**article 5 *bis***) ;

– définition des notions « d'agent agissant pour le compte des bureaux d'enregistrement » et de « résilience » et modification de la définition de la notion de « vulnérabilité » (**article 6**) ;

– exclusion de la liste des entités essentielles des entités dont les activités relèvent du secteur de la sécurité nucléaire, inclusion dans la liste des entités essentielles des entreprises éditrices de logiciels, de l'ensemble des communautés d'agglomération, des établissements publics de santé et des établissements et services sociaux et médico-sociaux (**article 8**) ;

– exclusion de la liste des entités importantes des entités dont les activités relèvent du secteur de la sécurité nucléaire, inclusion dans la liste des entités importantes de l'ensemble des communautés d'agglomération, des établissements publics de santé et des établissements et services sociaux et médico-sociaux (**article 9**) ;

– précision que l'élaboration de la liste des entités essentielles et importantes doit être faite après avis des ministères compétents et possibilité pour le premier ministre d'exempter par arrêté certaines entités exerçant des missions régaliennes de certaines obligations prévues par les articles 14 et 17 du projet de loi (**article 10**) ;

– mise en œuvre à leurs frais par les entités des mesures techniques, opérationnelles et organisationnelles, précision que les mesures précitées garantissent un niveau de résilience adapté et proportionné au risque, inscription de critères pour déterminer les mesures de cybersécurité prises par les entités critiques (**article 14**) ;

– clarification des conditions dans lesquelles seront reconnues les normes et spécifications techniques permettant aux entités régulées de démontrer leur conformité aux objectifs visés et facilitation pour les entités établies dans plusieurs pays au sein de l'Union européenne de la reconnaissance de leur conformité lorsqu'elles appliquent un autre référentiel que celui de l'ANSSI (**article 15**) ;

– élargissement du champ de l'article 16 *bis* pour inclure, au-delà des outils techniques, les « processus » permettant un accès non consenti aux données protégées (**article 16 *bis***) ;

– précision qu'un incident est considéré comme important uniquement s'il a causé des pertes financières significatives (**article 17**) ;

– précision que, dans le cadre d'infractions au droit de la propriété intellectuelle, deux catégories d'agents doivent être spécialement habilités pour solliciter un accès aux données d'enregistrement des noms de domaines : les agents assermentés et les commissaires de justice (**article 22**) ;

– suppression de la notion d'intérêts commerciaux afin de permettre le partage d'informations entre les autorités compétentes (**article 23**) ;

– suppression de la certification par l'ANSSI des services de coffre-fort numérique (**article 26 A**) ;

– possibilité de soumettre aux contrôles de l'ANSSI les OIV qui ne sont pas déjà soumis à son contrôle en tant qu'entité essentielle ou importante (**article 26**) ;

– introduction d'un critère de nécessité pour apprécier la légalité des demandes d'accès aux systèmes d'information appartenant aux entités contrôlées dans le cadre d'un contrôle diligenté par l'ANSSI et ouverture de la possibilité pour les agents en charge des contrôles de prélever des échantillons de produits (**article 27**) ;

– distinction des montants des sanctions financières entre les entités essentielles et les entités importantes (**article 28**) ;

– possibilité pour les entités mentionnées à l'article 14 du projet de loi de choisir les prestataires de services certifiés, qualifiés ou agréées ou organismes indépendants sur la base d'une liste élaborée par l'ANSSI (**article 29**) ;

– possibilité d'une procédure dématérialisée pour l'établissement ou la conversion des actes établis par les agents en charge des contrôles (**article 33 *bis***) ;

– possibilité de nommer une personnalité qualifiée au sein de la commission des sanctions si celle-ci a exercé au cours des trois années précédentes une activité au sein de l'ANSSI ou au sein d'entités essentielles ou importantes (**article 36**) ;

– octroi par l'ANSSI aux organismes d'évaluation du pouvoir d'évaluation de la conformité à des exigences de cybersécurité et à la délivrance de certificats de conformité (**article 37 *bis***).

C. TITRE III

Au **chapitre I^er^**, les principaux apports de la commission spéciale ont été les suivants :

– transmission à l'Agence nationale de sécurité des systèmes d'information (ANSSI) des déclarations d'incidents majeurs liés aux technologies de l'information et de la communication (TIC) et des notifications volontaires de cybermenaces importantes reçues par l'Autorité de contrôle prudentiel et de résolution (ACPR) de la part des entités financières considérées comme essentielles ou importantes au sens de la directive NIS 2 (**article 43 A**) ;

– transmission également à l'ANSSI de celles reçues par l'Autorité des marchés financiers (AMF) au moyen d'un document commun (**article 45 *bis***).

Au **chapitre II**, la commission spéciale a réécrit l'**article 58 *bis*** afin que l'inversion de la charge de la preuve en cas d'attaque informatique soit effectivement inversée vis-à-vis des assurances.

Parmi les dispositions finales du **chapitre V**, la commission spéciale a rétabli une entrée en application différenciée des nouvelles exigences prudentielles propres aux prestataires de services bancaires pour les sociétés de financement selon leur taille (**article 62**). Elles entreront en vigueur dès le lendemain de la promulgation de la loi pour les plus grandes d'entre elles tandis que celles « de petite taille et non complexes », au sens du droit de l'Union européenne, ne devront s'y conformer que d'ici le 17 janvier 2027, soit un an de plus que ce que prévoyait le projet de loi dans sa rédaction initiale.

La commission spéciale a également adopté deux articles additionnels relatifs à des demandes de rapport :

– sur les moyens nécessaires à l'ANSSI pour s'assurer de la mise en œuvre de la transposition de la directive NIS 2 (**article 63**) ;

– au sujet de la mise en œuvre de la stratégie nationale en matière de cybersécurité dont l'élaboration est prévue à l'article 5 *bis* (**article 64**).

Enfin, les membres de la commission spéciale ont adopté divers amendements rédactionnels et ont étendu l'application des articles additionnels par

rapport au projet de loi initial en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

*

* *

COMMENTAIRE DES ARTICLES

TITRE IER
RÉSILIENCE DES ACTIVITÉS D'IMPORTANCE VITALE

CHAPITRE IER
DISPOSITIONS GÉNÉRALES

Article 1er

(art. L. 1332-1 à 6 et art. L. 1332-7 à 22 [nouveaux] du code de la défense)

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

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article transpose en droit national la directive 2022/2557 du Parlement et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, dite directive REC. L'article actualise le dispositif de sécurité des activités d'importance vitale (SAIV) prévu dans le code de la défense depuis 2006. Les principales modifications apportées à ce dispositif sont les suivantes :

– les opérateurs d'importance vitale (OIV) seront tenus d'analyser les risques de toute nature auxquels ils font face et d'analyser leurs dépendances à l'échelle de l'opérateur, et non plus seulement des points d'importance vitale (PIV) ;

– un plan de résilience opérateur (PRO) fusionne le plan de sécurité opérateur (PSO) et le plan de continuité de l'activité (PCA), qui existent actuellement ;

– le plan particulier de résilience (PPR) se substitue au plan particulier de protection (PPP) ;

– une astreinte pourra être imposée aux opérateurs qui refusent de se mettre en conformité avec leurs obligations ;

– le champ des enquêtes administratives pour contrôler l'accès aux sites est étendu aux accès à distance et l'avis de l'autorité administratif passe de simple à conforme ;

– les OIV devront signaler les incidents à l'autorité administrative compétente – préfecture de département et secrétariat général de la défense et de la sécurité nationale (SGDSN), qui pourra en informer le public ;

– la notion d'entité critique d'importance européenne particulière est introduite en droit national, avec la possibilité de solliciter des missions de conseil de la Commission européenne auprès de ces entités ;

– une commission des sanctions est instituée pour réprimer les manquements des opérateurs au dispositif, à la place des sanctions pénales actuellement prévues ;

– les OIV pourront recourir à des régimes dérogatoires aux marchés publics ou aux contrats de concession, pour lutter contre des tentatives d'ingérence étrangères.

En outre, la transposition de la directive se traduit par un élargissement des secteurs couverts par le dispositif à l'assainissement de l'eau, aux réseaux de chaleur et de froid et à l'hydrogène.

➢ **Dernières modifications législatives intervenues**

Le dispositif de SAIV a été institué par l'ordonnance n° 2004-1374 du 20 décembre 2004 relative à la partie législative du code de la défense, sur la base de l'ancien dispositif de protection des points et réseaux sensibles datant de l'ordonnance n° 58-1371 du 29 décembre 1958 tendant à renforcer la protection des installations d'importance vitale.

L'article 3 de la loi n° 2005-1550 du 12 décembre 2005 a précisé que les dispositions entraient en vigueur à compter de la désignation de l'autorité administrative compétente. Cette autorité administrative, le préfet de département, a été désignée par le décret n° 2006-212 du 23 février 2006.

L'article 22 de la 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 a déplacé les articles régissant le dispositif dans le code de la défense, au sein d'une nouvelle section 1 au chapitre II du titre III du livre III.

➢ **Modifications apportées par le Sénat**

Outre des amendements rédactionnels, le Sénat a apporté les modifications suivantes :

– la notion d'incident (alinéa 12) et celle de résilience (alinéa 13) ont été définies ;

– l'astreinte journalière a été précisée comme s'appliquant 24 heures après la mise en demeure ;

– la notification d'incidents à l'autorité administrative devra intervenir au plus tard 24 heures après la notification et un décret en Conseil d'État précisera les conditions de mise en œuvre de l'obligation de notification (alinéa 46) ;

– les conditions de saisine de la Commission européenne pour effectuer une mission de conseil ont été précisées (alinéa 53) ;

– l'applicabilité du moyen de démontrer la conformité aux règles de sécurité, prévue à l'article 15 du présent projet de loi, a été étendue aux opérateurs d'importance vitale qui ne sont soumis ni à la directive 2022/2555 NIS 2 ni à la directive REC ;

– les personnalités qualifiées membres de la commission des sanctions seront nommées par le premier ministre, le président de l'Assemblée nationale et le président du Sénat (alinéa 83), et pas seulement par le premier ministre.

➢ **Modifications apportées par la commission**

Au-delà de plusieurs amendements rédactionnels, la commission spéciale a apporté plusieurs modifications à l'article 1er :

– clarification entre la notion d'infrastructure critique utilisée en droit européen et celle de point d'importance vitale utilisée en droit national (alinéa 9) ;

– extension de l'analyse des dépendances aux sous-traitants, selon un délai fixé par voie réglementaire, et aux vulnérabilités envers les fournisseurs de solutions logicielles et matérielles propriétaires (alinéa 32) ;

– distinction dans le plan de résilience entre les dispositifs et les dispositions de résilience (alinéa 35) ;

– ajout de l'avis de la Commission nationale de l'informatique et des libertés (CNIL) sur le décret en Conseil d'État précisant les modalités de l'avis de l'autorité administrative sur une autorisation d'accès à un point d'importance vitale (alinéa 40) ;

– mise en cohérence des obligations imposées aux OIV avec celles prévues par la directive NIS 2 (alinéa 60) ;

– nomination des personnalités qualifiées de la commission des sanctions par le premier ministre, plutôt que par le premier ministre, le président de l'Assemblée nationale et le président du Sénat (alinéa 83) ;

– inscription dans le code de la défense du caractère contradictoire de la procédure devant la commission des sanctions (alinéa 87) ;

– mandat non renouvelable des membres, hors personnalités qualifiées, de la commission des sanctions (alinéa 90).

1. L'état du droit : la France est dotée d'un dispositif destiné à assurer la sécurité des activités d'importance vitale

a. Le dispositif de SAIV garantit la protection d'environ 1 500 points d'importance vitale pour la nation

Le dispositif de sécurité des activités d'importance vitale mis en place en 2006 vise à garantir la protection des points d'importance vitale, c'est-à-dire les installations et ouvrages essentiels pour garantir le potentiel économique et militaire ainsi que la survie de la nation. Prévu aux articles L. 1332-1 à L. 1332-7 du code de la défense, le dispositif s'applique aux opérateurs d'importance vitale, publics et privés, qui exploitent les établissements et ouvrages dont l'indisponibilité menacerait la continuité de la vie de la nation ou qui pourraient constituer un danger grave pour la population. Les établissements sensibles peuvent être des hôpitaux, des usines, des locaux d'administration, des bases militaires etc.

Un arrêté du premier ministre du 2 juin 2006 [(1)], modifié par un arrêté du 3 juillet 2008, fixe la liste des douze secteurs d'importance vitale couverts par ce dispositif, qui concerne environ 300 OIV et 1 500 PIV, dont environ 40 OIV dans le secteur de la défense. Ces secteurs ont trait à la production de biens et services indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la nation. Chaque secteur est supervisé par un ministre coordonnateur. Le critère clé d'identification d'un opérateur est celui de la non redondance : en cas de défaillance, l'absence des activités de l'opérateur menacerait la continuité de la vie de la nation.

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

LISTE DES SECTEURS COUVERTS PAR LE DISPOSITIF ET DES MINISTÈRES COORDONNATEURS

Secteurs	Ministre coordonnateur
Activités civiles de l'État	Intérieur
Activités judiciaires	Justice
Activités militaires de l'État	Défense
Alimentation	Agriculture
Communications électroniques, audiovisuel et informatique	Communications électroniques
Énergie	Énergie
Espace et recherche	Recherche
Finances	Économie et finances
Gestion de l'eau	Écologie
Industrie	Industrie
Santé	Santé
Transports	Transports

Source : étude d'impact, page 11.

Les interlocuteurs auditionnés par la rapporteure Catherine Hervieu soulignent l'efficacité et la robustesse du dispositif, qui a fait ses preuves face à la menace terroriste ou à l'occasion des Jeux olympiques et paralympiques de Paris. Le dispositif a permis de créer une culture de la sécurité au sein des entreprises et des établissements publics, avec une logique d'anticipation des risques et de protection des sites sensibles (notion de « points fortifiés »). Il repose sur la collaboration entre les services de l'État et les opérateurs au travers d'un accompagnement de la part de l'autorité administrative.

b. Le dispositif de SAIV repose sur les directives nationales de sécurité et l'élaboration de plans par les opérateurs

L'instruction générale interministérielle n° 6600 relative à la sécurité des activités d'importance vitale du 7 janvier 2014 fixe les modalités de mise en œuvre du dispositif.

Une directive nationale de sécurité (DNS) s'applique à tout ou partie d'un secteur d'importance vitale. Elle décrit le périmètre, identifie les responsables et détermine le besoin de sécurité et les politiques associées. Elle définit des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste.

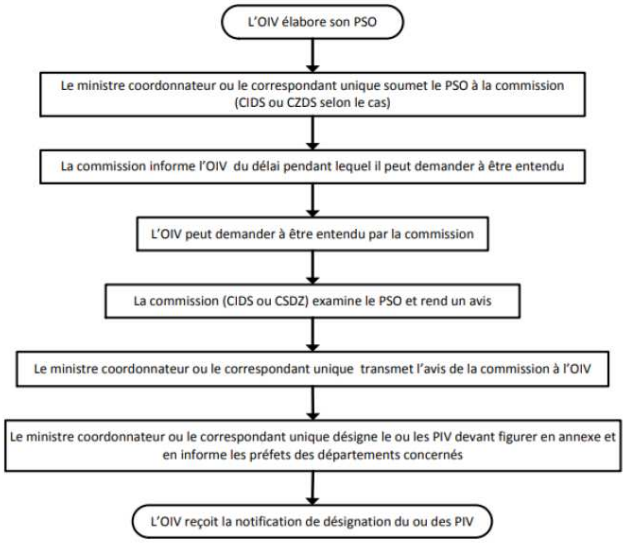
Désignés par l'État, les opérateurs d'importance vitale sont tenus de garantir à leurs frais la sécurité de leurs sites à travers des documents de planification. Ils doivent identifier les PIV, analyser les risques pouvant menacer leur activité, décliner des mesures de sauvegarde et désigner un délégué à la défense et la sécurité (DDSS), habilité au secret de la défense nationale. Le DDSS est l'interlocuteur de l'administration pour tout ce qui a trait au dispositif.

L'opérateur doit élaborer un plan particulier de protection (PPP) pour chaque PIV, un plan de continuité de l'activité (PCA) et un plan de sécurité opérateur (PSO). Ce dernier est obligatoire si l'opérateur a plus d'un PIV. Le plan

de protection externe est élaboré par le préfet de département en complément de chaque PPP.

Le PSO décrit l'organisation et la politique de sécurité d'un OIV. Il repose sur une analyse des risques et doit permettre à l'opérateur de s'approprier la DNS. Les plans particuliers de protection y sont annexés. Le PSO n'est aujourd'hui évoqué que dans la partie réglementaire du code de la défense (articles R. 1332-19 et suivants). Il s'agit d'un document classifié et approuvé par arrêté du ministre coordonnateur. L'opérateur dispose d'un délai de 6 mois à compter de la réception de la DNS pour élaborer le PSO et le transmettre au ministère coordonnateur.

Processus d'élaboration d'un plan de sécurité opérateur, hors secteur de la défense



NB : Ce processus ne s'applique pas au PSO d'un opérateur relevant du ministre de la défense.

Source : étude d'impact, page 73.

Le PCA décline la stratégie d'ensemble pour assurer la continuité de l'activité de l'OIV. Le PCA n'est pas classifié et n'est pas validé par l'autorité administrative.

Le PPP est établi pour chaque PIV. Il précise les mesures de protection. Il décrit les moyens utilisés pour retarder et mettre en échec les tentatives malveillantes et faciliter le rétablissement de l'activité. C'est un document comprenant 50 à 100 pages, approuvé par arrêté du préfet de département.

Un PPE, élaboré par les pouvoirs publics, complète le PPP en précisant les modalités d'intervention des forces de sécurité, sous l'autorité du préfet de département. Document classifié, il décrit les moyens humains et matériels nécessaires. Le document comprend une quinzaine de pages. Les services du haut fonctionnaire de défense et de sécurité (HFDS) auditionnés ont indiqué que le taux de complétion des PPE est relativement modéré.

c. Le dispositif est coordonné par le SGDSN, animé par le ministre coordonnateur pour son secteur et décliné à l'échelle territoriale par le préfet de zone de défense et de sécurité

Le premier ministre définit le cadre général du dispositif. Il est chargé de fixer la liste des secteurs soumis à cette réglementation, de désigner pour chacun d'entre eux un ministre coordonnateur et de déterminer une méthode à suivre pour déterminer, pour chaque secteur, les scénarios de menaces et les PSO types pour y remédier. Il approuve par arrêté les DNS.

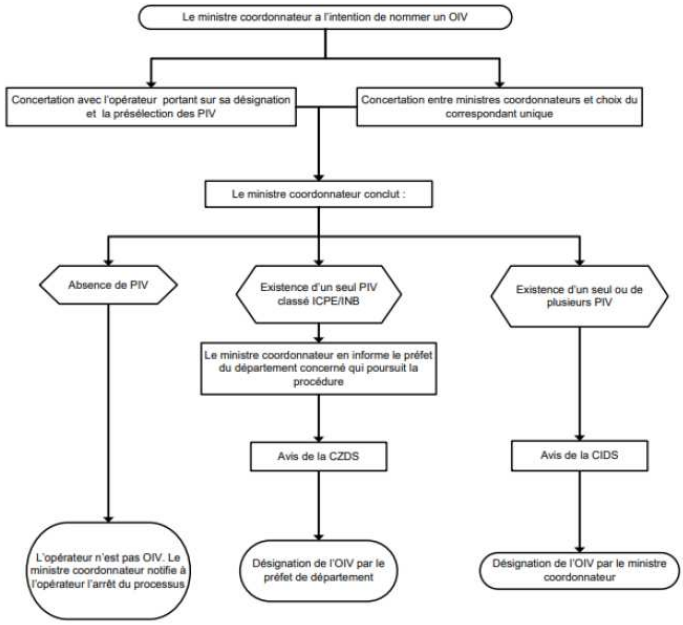
Le SGDSN coordonne le dispositif de SAIV au niveau national, au nom du premier ministre. Il assure la présidence et le secrétariat de la commission interministérielle de défense et de sécurité (CIDS), dont le rôle est consultatif et qui se réunit deux fois par an. La commission est sollicitée pour avis sur la désignation des OIV, les DNS, les PSO et la liste des PIV fournie par les OIV. La commission ne rend pas d'avis sur les OIV, les DNS et les PIV du secteur de la défense, qui relèvent du seul ministère de la défense, en raison de la confidentialité des activités.

Le ministre coordonnateur veille à l'application du dispositif dans les secteurs d'activité de son champ de compétences. Il désigne les OIV pour son secteur après avis de la CIDS, instruit les PSO et les approuve par arrêté. Il désigne les PIV, sur proposition des OIV (hors PIV classés ICPE [1] ou comprenant une installation nucléaire de base [2] dont la désignation revient alors au préfet de département). Il élabore la DNS puis, après approbation par le premier ministre, la diffuse aux préfectures de zone et aux services déconcentrés de son ministère. L'animation de la mise en œuvre du dispositif est assurée par les services du HFDS ; pour la défense, il s'agit de la direction de la protection des installations, moyens et activités de la défense (DPID). Le ministère chargé de l'économie et des finances est responsable d'environ 20 % des OIV et celui de la transition écologique de 50 %.

(1) Installations classées protection de l'environnement, art. L. 511-1 du code de l'environnement.

(2) Art. L. 593-2 du code de l'environnement

PROCESSUS DE DÉSIGNATION D'UN OIV INITIÉ PAR UN MINISTRE COORDONNATEUR



Source : étude d'impact, page 59.

Le préfet de zone de défense et de sécurité est responsable de coordonner le dispositif à l'échelle territoriale, avec le soutien du préfet délégué pour la défense et la sécurité. Le préfet préside la commission zonale de défense et de sécurité (CZDS), qui contrôle les PIV sur le ressort territorial de la zone de défense. La CZDS exerce les mêmes fonctions que la CIDS pour les OIV qui ne sont présents que sur une seule zone de défense et de sécurité. Des agents du service du HFDS pour les ministères de l'économie et des finances (1) et de la transition écologique (2) sont rattachés aux préfectures de zone pour faire le lien entre l'échelon territorial et les ministères coordonnateurs.

Les préfets de département supervisent l'application des mesures pour les PIV de leur département, approuvent les PPP (hors secteur de la défense) après avis de la CZDS et planifient les moyens d'intervention de l'État avec les plans de protection externe (PPE). Ils peuvent initier la nomination d'un OIV.

(1) Il y a 16 chargés de mission sécurité économique (CMSE) : 1 dans chaque zone de défense et de sécurité métropolitaine, 1 en Martinique pour la zone Antilles, 1 à La Réunion pour la zone de l'océan Indien.

(2) Adjoint sécurité défense en direction régionale de l'environnement, de l'aménagement et du logement de zone.

2. Le dispositif proposé : une actualisation du dispositif de SAIV qui tire les conséquences de la directive REC

a. La révision du dispositif est rendue nécessaire par la directive européenne sur la résilience des activités critiques (REC)

La directive du 8 décembre 2008 [(1)] a introduit en droit européen la notion d'infrastructure critique européenne (ICE), en se limitant à recenser les infrastructures dans les secteurs de l'énergie et des transports et à prévoir leur protection physique par les États membres. Une ICE est une infrastructure située dans un État membre dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins. La directive était doublement limitée, par son périmètre d'abord, car elle se limitait à deux secteurs et aux entités de dimension européenne, et par ses obligations ensuite, la protection physique des infrastructures critiques relevant des États membres et des opérateurs.

Une évaluation menée par la Commission européenne en 2019 a souligné la nécessité de mettre à jour le dispositif, volonté accrue par la pandémie de Covid de 2020. La Commission a indiqué sa volonté de passer d'une logique d'infrastructures à celle d'entités, comprenant aussi les services associés, et de renforcer les règles ayant trait à résilience des entités critiques.

La directive de 2022 sur la résilience des entités critiques (dite directive REC), négociée sous présidence française de l'Union européenne, élargit le champ de la résilience des opérateurs aux entités critiques nationales, au-delà des seules infrastructures critiques européennes, et fixe des standards minimums de résilience (article 3 de la directive). Elle s'inscrit dans une politique de résilience globale puisque les entités seront également soumises aux obligations de cyber-résilience prévues par la directive NIS 2 [(2)] . Le texte final constitue une position d'équilibre entre des enjeux de souveraineté et une volonté de la Commission européenne de disposer d'un fort niveau d'harmonisation et de partage d'information entre les États membres de l'Union. La directive REC devait être transposée au sein des États membres au plus tard le 17 octobre 2024 (article 26), comme la directive NIS 2.

Une entité critique désigne toute entité publique ou privée désignée par un État membre et opérant dans un secteur stratégique. Une entité est qualifiée « d'importance européenne particulière » si elle opère des services similaires dans moins six États membres. La résilience est entendue comme la capacité d'une entité à prévenir tout incident, à s'en protéger, y réagir, l'atténuer, l'absorber et s'en rétablir. La criticité des entités est évaluée à l'aune de plusieurs critères précisés à l'article 7 de la directive REC : le nombre d'utilisateurs tributaires du service, l'impact potentiel des incidents sur les activités économiques et sociétales, la part de marché, la zone géographique couverte, l'existence de solutions de rechange pour fournir le service essentiel. À l'inverse, une clause de sauvegarde permet aux États membres de ne pas appliquer certaines dispositions aux entités liées à la défense ou à la sécurité nationale.

---

(1) Directive 2008/114/CE concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

(2) 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.

L'objet de la directive REC est d'établir des règles minimales harmonisées pour garantir la fourniture, dans le marché intérieur, des services considérés comme essentiels au maintien de fonctions sociétales ou économiques vitales. La directive impose par conséquent des obligations aux États membres et aux entités critiques. Elle crée un cadre pour traiter de manière globale la résilience des entités critiques en ce qui concerne tous les risques, qu'ils soient naturels, d'origine humaine, accidentels ou intentionnels. La directive vise également à améliorer la coopération transfrontalière, en évitant le *dumping* réglementaire et en améliorant la prise en compte des entités critiques qui opèrent dans plusieurs États membres.

Les États membres doivent :

– développer une stratégie nationale pour renforcer la sécurité des entités critiques, en s'appuyant quand c'est possible sur les stratégies sectorielles et les plans existants (art. 4) ;

– recenser les entités critiques qui seront soumises à des exigences de résilience (art. 6) et les aider à s'acquitter de leurs obligations (art. 10) ;

– évaluer les risques auxquelles les entités critiques peuvent être exposées (art. 5) ;

– communiquer à la Commission européenne la liste des services essentiels et le nombre d'entités critiques ;

– désigner des autorités chargées de surveiller l'application de cette directive (art. 9) et faire en sorte qu'elles disposent des pouvoirs adéquats (art. 21) ;

– préciser les conditions dans lesquelles les entités critiques peuvent demander des vérifications des antécédents auprès des autorités (art. 14) ;

– déterminer un régime de sanctions pour assurer la mise en œuvre du dispositif (art. 22).

Les entités critiques doivent, quant à elles, procéder à une évaluation des risques auxquelles elles sont exposées et qui pourraient perturber leur fourniture de services essentiels (art. 12). Elles doivent ensuite mettre en œuvre des mesures techniques, de sécurité et organisationnelles de manière à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber et à s'en remettre (art. 13). Ces mesures doivent figurer dans un plan de résilience et inclure des mécanismes de notification des incidents aux pouvoirs publics (art. 15).

Enfin, la directive identifie les entités critiques d'importance européenne particulière, qui fournissent des services essentiels à ou dans au moins six États membres de l'Union (art. 17).

CORRESPONDANCE ENTRE LES ARTICLES DE LA DIRECTIVE ET CEUX DU CODE DE LA DÉFENSE INTRODUITS PAR LE PROJET DE LOI

Dispositif	Article de la directive REC	Article du code de la défense
Définitions	2	1332-1 (modifié)
Entité critique	1	1332-2 (modifié)
Évaluation des risques	12	1332-3 (modifié)
Mesures de résilience	13	1332-3 (modifié)
Analyse des dépendances	4, 12 et 19	1332-4 (modifié)
Plan particulier de résilience	13	1332-5 (modifié)
Enquêtes administratives de sécurité	14	1332-6 (modifié)
Notification des incidents	15	1332-7 (nouveau)
Entité critique d'importance européenne particulière	17	1332-8 (nouveau)
Missions de conseil de la Commission	18	1332-9 (nouveau)
Habilitation et contrôle des agents	21	1332-12 à 14 (nouveaux)
Régime de sanctions	22	1332-15 à 19 (nouveaux)

La directive REC s'applique à onze secteurs listés en annexe de la directive, chacun comprenant plusieurs sous-secteurs : énergie, transports, bancaire, infrastructure des marchés financiers, santé, eau potable, eaux résiduaires, infrastructures numériques, administration publique, espace, denrées alimentaires. Le règlement délégué 2023/450 de la Commission du 25 juillet 2023 identifie les services essentiels dans les secteurs et sous-secteurs couverts par la directive.

La transposition de la directive REC devrait se traduire, selon l'étude d'impact, par un élargissement du dispositif de SAIV à trois sous-secteurs : réseaux de chaleur et de froid (service essentiel n° 1b), hydrogène (n° 1e) et assainissement de l'eau (n° 6). Les associations représentatives de ces secteurs ont été auditionnées par la rapporteure Catherine Hervieu. Selon le HFDS du ministère de la transition écologique, cela correspond à une hausse d'une dizaine de nouveaux OIV. Les réseaux de chaleur et de froid sont des infrastructures locales qui desservent des bâtiments ou des quartiers. Selon la FEDENE, la France métropolitaine compte environ 1 000 réseaux de chaleur et de froid, de dimensions très hétérogènes. Seuls quelques réseaux de très grande taille devraient être assujettis au dispositif.

Le titre I^{er} du projet de loi vise ainsi à transposer la directive REC en révisant le dispositif national pour y intégrer les obligations prévues par la directive et étendre son champ d'application. La transposition de la directive repose sur une révision du dispositif actuel et non sur une refonte du dispositif national. Il acte le passage de la protection des « points fortifiés » à la résilience des entités. Les hauts fonctionnaires de défense et de sécurité ont rappelé dans leur audition la possibilité, avec cette révision, de faire face plus efficacement à des nouvelles menaces : dépendance énergétique, cyber, changement climatique, souveraineté numérique, sécurité économique.

PLANS AVANT ET APRÈS L'ENTRÉE EN VIGUEUR DU PROJET DE LOI

Plan actuel	Nouveau plan
Plan de sécurité opérateur (PSO)	Plan de résilience opérateur (PRO)
Plan de continuité de l'activité (PCA)	
Plan particulier de protection (PPP)	Plan particulier de résilience (PPR)
Plan de protection externe (PPE)	Plan particulier de résilience (PPR)

b. Articles L. 1332-1 et L. 1332-2 (modifiés) : définitions

L'article 1er du projet de loi introduit plusieurs définitions principales pour mettre en conformité le droit national avec le droit européen :

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

– infrastructure critique (**alinéa 8**) : « 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 ». Le texte distingue les points d'importance vitale et les systèmes d'information d'importance vitale.

– opérateurs d'importance vitale (**alinéas 14 à 17**, qui modifient l'article L. 1332-2 du code de la défense) : il s'agit des opérateurs qui exercent une activité d'importance vitale au moyen d'une infrastructure critique.

Le champ des OIV retenu dans la transposition est plus large que celui des entités critiques au sens de la directive car il inclut les opérateurs régaliens du secteur de la défense et de la sécurité de la nation, exclus du champ de la directive REC (art. 1er, alinéa 6). L'entrée en vigueur du texte devrait conduire à augmenter le nombre d'OIV et de PIV d'une dizaine selon le SGDSN, même si le nombre exact est couvert par le secret de la défense nationale.

Il revient à l'autorité administrative de préciser les activités d'importance vitale exercées par un opérateur qui relèvent du champ des services essentiels, et ainsi les opérateurs qui doivent être considérés comme des entités critiques au sens de la directive (**alinéa 16**).

Comme dans le dispositif actuel de SAIV, l'ensemble des obligations imposées aux OIV est à la charge financière des opérateurs (**alinéa 18**).

c. Article L. 1332-3 (modifié) : évaluation des risques, mesures de résilience et plan de résilience opérateur des OIV

Les OIV seront tenus d'évaluer les risques de toute nature (**alinéa 22**), dans un délai de neuf mois à compter de la désignation comme OIV, conformément au paragraphe 1 de l'article 12 de la directive REC. Cette évaluation devra être actualisée au moins tous les quatre ans (**alinéa 23**). Le SGDSN a précisé que les

nouveaux opérateurs assujettis seront, pour la plupart, informés en amont de leur désignation formelle comme OIV, pour leur laisser le temps de désigner un DDSS qui sera en charge du dispositif.

À partir de cette analyse des risques, les OIV devront prévoir des mesures de résilience technique, opérationnelle et organisationnelle pour assurer la continuité de leur opération (**alinéa 24**). Un décret en Conseil d'État précise la nature des mesures de résilience pour chaque catégorie d'OIV (**alinéa 31**).

Actuellement, la partie législative du code de la défense dispose seulement que les opérateurs sont tenus de prévoir des mesures de protection au niveau des PIV, tandis que l'évaluation des risques relève de la partie réglementaire. Ce nouvel article L. 1332-3 permet ainsi de faire entrer dans la loi les obligations d'analyse de risque et de plan de résilience.

L'analyse des risques des OIV et les mesures pour y faire face devront être détaillées dans un plan de résilience opérateur (PRO, **alinéa 25**). Le PRO, prévu à l'article 13 de la directive REC, fusionnera le plan de sécurité opérateur et le plan de continuité de l'activité qui existent aujourd'hui. Le PCA actuel n'étant validé qu'à l'échelle de l'opérateur, la création du PRO fera donc entrer dans le champ de l'autorité administrative la continuité de l'activité. Établi dans les dix mois après la désignation comme OIV, le plan sera approuvé par l'autorité administrative (**alinéa 25**).

L'autorité administrative pourra décider qu'un document déjà existant tienne lieu de PRO (**alinéa 26**), ce qui permettra aux opérateurs déjà assujettis de se conformer plus facilement à leurs obligations. Toutefois, les PSO actuels devront être *in fine* mis à jour pour se conformer aux nouveaux plans-types.

Les associations professionnelles (FEDENE, FP2E) ainsi que la DPID, auditionnées par la rapporteure Catherine Hervieu, ont exprimé une inquiétude sur la capacité des opérateurs à respecter les délais imposés par le projet de loi. Aujourd'hui, il s'écoule entre deux et trois ans entre la désignation d'un OIV et la validation définitive des PPR par le ministère coordonnateur, dont un an et demi pour la validation du PSO. Le délai légal, de 39 mois, va être réduit à 10 mois avec le nouveau dispositif.

Si l'opérateur refuse d'élaborer un PRO, l'autorité administrative pourra lui adresser une mise en demeure pour élaborer le plan ou le modifier, dans un délai qui devra être supérieur à un mois (**alinéa 28**). La mise en demeure pourra être assortie d'une astreinte d'un montant de 5 000 euros par jour de retard.

Alors que le régime de sanctions administratives introduit par le présent projet de loi aux alinéas 76 à 97 exclut explicitement les établissements publics, l'État et les collectivités territoriales (**alinéa 91**), ces derniers ne sont pas exclus du dispositif d'astreinte.

d. Article L. 1332-4 (modifié) : analyse des dépendances

Les OIV devront également, dans un délai de neuf mois à compter de leur désignation, réaliser une analyse de leurs dépendances à l'égard de tiers, y compris dans leur chaîne d'approvisionnement (**alinéa 32**).

e. Article L. 1332-5 (modifié) : établissement d'un plan particulier de résilience

Les alinéas 34 à 37 modifient l'article L. 1332-5 du code de la défense et fixent l'obligation aux OIV d'établir un plan particulier de résilience (PPR) pour chaque PIV, qui se substitue au plan particulier de protection (PPP). Comme pour le PSO, l'autorité administrative pourra reconnaître comme équivalent au PPR un document existant (**alinéa 36**). Le PPR, comme précisé dans l'étude d'impact, a vocation à intégrer en annexe ce qui figure actuellement dans le PPE. L'objectif est d'appréhender la sécurité des PIV dans une approche globale, où les services de l'État et l'opérateur œuvrent de concert, justifiant un document unique.

Ce nouveau plan constitue une obligation supplémentaire par rapport à la directive REC qui fixe au niveau de l'opérateur seulement l'obligation d'élaborer un plan de résilience.

Si l'opérateur refuse d'élaborer le PPR, l'autorité administrative pourra lui adresser une mise en demeure pour élaborer le plan ou le modifier, dans un délai qui devra être supérieur à un mois (**alinéa 37**). La mise en demeure pourra être accompagnée d'une astreinte d'un montant de 5 000 euros par jour de retard.

f. Article L. 1332-6 (modifié) : enquêtes administratives de sécurité

Les **alinéas 40 à 45** modifient l'article L. 1332-6 du code de la défense en actualisant le dispositif de contrôle des sites vitaux. La loi du 14 mars 2011 dite LOPPSI 2 [(1)] a institué la possibilité pour les OIV de demander un avis à l'autorité administrative pour contrôler l'accès des individus aux PIV. Cette faculté est inscrite aujourd'hui à l'article L. 1332-2-1 du code de la défense. L'avis est rendu à la suite d'une enquête administrative qui peut donner lieu à la consultation du casier judiciaire et de traitements automatisés de données à caractère personnel.

(1) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

En pratique, le service national des enquêtes administratives de sécurité (SNEAS), saisi pour tous les sites des opérateurs civils par les préfectures, estime à 70 000 le nombre d'enquêtes annuelles réalisées pour les points d'importance vitale. Le service estime qu'entre 1 et 2 % de ces enquêtes donnent lieu à un avis négatif. La direction du renseignement et de la sécurité de la défense (DRSD), saisie pour tous les sites relevant du ministère chargé de la défense, réalise les enquêtes annuelles pour les PIV relevant de leurs secteurs d'activités et pour les besoins du ministère. Dans le secteur de la défense, la DPID a indiqué que l'ensemble des accès sont déjà couverts par une obligation d'enquête administrative. Le SGDSN a précisé que le volume d'activité supplémentaire était en cours d'évaluation.

Le dispositif prévu élargit le champ des enquêtes aux accès à distance et acte le passage d'une logique d'avis simple à celle d'un avis conforme lorsque l'avis est négatif. Conformément à l'article 14 de la directive REC, le PRO devra ainsi prévoir :

– les cas dans lesquels l'avis peut être sollicité avant d'accorder une autorisation d'accès physique ou à distance aux points d'importance vitale et aux systèmes d'information (**alinéa 43**) ;

– les fonctions sensibles qui peuvent nécessiter un avis avant le recrutement ou l'affectation d'une personne (**alinéa 42**).

La personne concernée est avertie de l'enquête dont elle fait l'objet (**alinéa 44**). Un avis défavorable est émis si le comportement de la personne est de nature à porter atteinte à l'exercice d'une activité d'importance vitale ou à la sécurité d'une infrastructure critique (**alinéa 45**).

En cas d'avis défavorable, l'opérateur, s'il est une personne morale de droit privé, est tenu de refuser l'autorisation (**alinéa 45**). La personne publique pourra directement refuser l'autorisation, ce qui constitue une mesure de police administrative.

Les administrations auditionnées par la rapporteure Catherine Hervieu ont mis en évidence plusieurs difficultés relatives à la logique d'avis conforme. La DGA souligne que la logique d'avis conforme pourra entrer en contradiction avec celle d'avis non conforme qui prévaut pour l'accès aux zones protégées (art. 413-7 du code pénal). Le service de HFDS du ministère de l'économie et des finances indique de son côté que l'avis obligatoire pourrait inciter des employeurs privés à formuler moins de demande d'avis, par crainte d'un refus. Le SNEAS admet que la procédure actuelle est parfois contournée, avec des départements qui ne formulent aucune demande d'enquête malgré la présence de PIV.

g. Article L. 1332-7 (nouveau) : notification des incidents

En application de l'article 15 de la directive REC, l'**alinéa 46** impose aux OIV de signaler à l'autorité administrative tout incident pouvant compromettre la continuité de leur activité. Un mécanisme de notification obligation était déjà prévu dans certains secteurs (télécommunications [(1)], nucléaire) et le présent article le généralise à l'ensemble des OIV.

L'**alinéa 47** prévoit la possibilité pour l'autorité administrative d'informer le public sur l'incident, si elle estime qu'il est dans l'intérêt général de le faire. Les autorités administratives auditionnées par la rapporteure Catherine Hervieu ont rappelé que cette possibilité sera utilisée au cas par cas, pour ne pas compromettre le secret de la défense nationale.

h. Article L. 1332-8 (nouveau) : entités critiques d'importance européenne particulière

Les **alinéas 48 à 52** introduisent la notion d'entités critiques d'importance européenne particulière qui figure à l'article 17 de la directive REC, à l'article L. 1332-8 du code de la défense. Comme indiqué dans la directive, il s'agit des OIV qui fournissent des services essentiels similaires dans au moins six États membres**.** La liste des services essentiels est précisée dans le règlement délégué 2023/450 du 25 juillet 2023 [(2)]. Les entités critiques d'importance européenne particulière sont tenues d'en informer l'autorité administrative au plus tard lors de l'approbation de leur plan de résilience (**alinéa 50**). La France notifiera ensuite à la Commission européenne l'existence d'une entité critique d'importance européenne.

Les obligations imposées aux entités critiques d'importance européenne particulière sont peu contraignantes, il s'agit d'accorder un accès en cas de mission de conseil de la Commission européenne prévue à l'article suivant du présent projet de loi, et à transmettre des informations supplémentaires à la Commission si nécessaire.

Les opérateurs relevant de la sécurité nationale, de la défense, du nucléaire ou de la répression pénale peuvent être exemptées des obligations incombant aux entités critiques d'importance européenne particulière (clause de sauvegarde), selon des modalités définies par un décret en Conseil d'État (**alinéa 52**). Le décret devrait prévoir que les PIV du secteur de la défense seront exonérés du mécanisme de remontée d'information à la Commission européenne prévu par la directive REC (art. 9, alinéa 3).

---

(1) Incident entraînant l'indisponibilité totale d'un service de communication concernant au moins 90 000 abonnés ou au moins 50 sites radio, et sur une durée de 2 heures.

(2) À noter que l'industrie est exclue du champ de la directive REC.

i. Article L. 1332-9 (nouveau) : missions de conseil de la Commission européenne

L'article L. 1332-9 du code de la défense, créé par les **alinéas 53 et 54**, permet à la Commission européenne d'effectuer des missions de conseil auprès des entités critiques d'importance européenne particulière. Cette disposition, issue de l'article 18 de la directive REC et conditionnée à l'accord de l'autorité administrative, permet à la Commission de fournir un avis sur le respect des obligations par l'opérateur et sur les moyens d'accroître sa résilience. À cette fin, l'opérateur est tenu de garantir l'accès aux informations, systèmes et installations, dans le respect du secret-défense (**alinéa 53**).

L'**alinéa 57** déplace les dispositions figurant actuellement à l'article L. 1332-6-1 A du code de la défense au sein d'un nouvel article L. 1332-10. Il s'agit de dispositions indépendantes de la directive REC qui autorisent les services de l'État à procéder à la captation, à l'enregistrement et à la transmission d'images à partir de caméras installées sur des aéronefs à des fins de protection des établissements et installations d'importance vitale. Il s'agit d'une simple modification de numérotation dans le cadre de la réécriture du chapitre II, sans modification sur le fond.

j. Article L. 1332-11 (nouveau) : systèmes d'information d'importance vitale

L'**alinéa 60** précise que les opérateurs relevant des obligations du titre I^er^ du présent projet de loi sont également assujettis aux obligations de cyber-résilience prévues par le titre II, qui transpose la directive NIS 2. Alors que les assujettis à REC sont également assujettis à NIS 2 en droit européen (considérant 30 de la directive NIS 2), le champ des OIV retenu dans le dispositif français étant plus large que celui de REC, il s'agissait d'acter ce changement de périmètre en droit national. C'est l'objectif du nouvel article L. 1332-11 du code de la défense, qui renvoie aux articles 14 à 16 et au premier alinéa de l'article 17 du projet de loi.

k. Articles L. 1332-12 à L. 1332-14 (nouveaux) : habilitations et contrôles des agents

Les articles L. 1332-12 à 14 du code de la défense, créés par les **alinéas 62 à 75**, définissent les prérogatives des agents chargés de contrôler les obligations des OIV. L'article L. 1332-12 prévoit que les agents désignés et assermentés selon des modalités prévues par un décret en Conseil d'État sont habilités à rechercher des manquements aux obligations incombant aux OIV, en dehors de celles résultant de la transposition de NIS 2.

En pratique, les visites sont effectuées par le préfet de département ou son représentant et des membres de la CZDS, accompagnés au besoin d'experts des services déconcentrés de l'État. L'équipe de contrôle est en général composée d'un représentant du préfet de zone de défense (chef de délégation), d'un représentant du

préfet de département, de la gendarmerie ou de la police, d'un représentant du ministère coordonnateur et d'experts de l'ANSSI.

Les agents disposent de prérogatives étendues prévues à l'article L. 1332-13. Ils peuvent ainsi (**alinéas 68 à 71**) :

– accéder aux locaux des OIV ;

– accéder à 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. À ce titre, ils peuvent exiger la communication de documents de toute nature propres à faciliter l'accomplissement de leur mission ;

– procéder, sur convocation ou sur place, à l'audition de toute personne susceptible d'apporter des éléments utiles à leurs constatations.

Les agents sont tenus au secret professionnel mais il ne peut leur être opposé (**alinéa 71**).

Le nouvel article L. 1332-14 précise qu'il est interdit de faire obstacle à l'exercice des fonctions des agents habilités (**alinéa 73**). Toute obstruction peut entraîner une sanction prononcée par la commission des sanctions d'un montant de dix millions d'euros ou pour une entreprise de 2 % du chiffre d'affaires mondial hors taxe de l'exercice précédent (**alinéa 74**).

l. Article L. 1332-15 à L. 1332-19 (nouveaux) : commission des sanctions

Les **alinéas 76 à 97** détaillent le nouveau dispositif de sanctions administratives, en remplacement des sanctions pénales prévues actuellement à l'article L. 1332-7 du code de la défense. En l'état actuel, le fait de se soustraire à une obligation incombant aux OIV est puni de 150 000 euros d'amende pour les dirigeants des opérateurs et de 750 000 euros pour les personnes morales. Les sanctions administratives doivent permettre une plus grande souplesse et une meilleure efficacité. Le SGDSN indique qu'aucune sanction n'a été prononcée depuis la mise en place du dispositif.

Si l'article 22 de la directive REC renvoie aux États membres la détermination du régime de sanctions applicables, la directive NIS 2 prévoit à son article 34 un régime de sanctions administratives. Or, comme les opérateurs d'importance vitale seront soumis aux sanctions administratives prévues par NIS 2, il apparaissait opportun de prévoir un régime analogue par souci de cohérence.

Une commission des sanctions est instituée auprès du premier ministre pour constater et sanctionner tout manquement aux obligations incombant aux OIV (art.

L. 1332-15 nouveau). Elle est composée : (i) d'un membre du Conseil d'État, président, désigné par le vice-président du Conseil d'État, (ii) d'un membre de la Cour de cassation désigné par le premier président de la Cour de cassation, (iii) d'un membre de la Cour des comptes désigné par le premier président de la Cour des comptes, (iv) de trois personnalités qualifiées nommées par le premier ministre, dans la version initiale du texte.

Ils exercent leurs fonctions en toute impartialité (**alinéa 85**). La commission statue par décision motivée, à la majorité des membres présents, après avoir entendu l'opérateur concerné (**alinéa 88**).

Le plafond de l'amende, fixé à l'article L. 1332-17 (nouveau), est de dix millions d'euros ou, lorsqu'il s'agit d'une entreprise, 2 % du chiffre d'affaires annuel mondial hors taxes de l'exercice précédent. Ces niveaux sont identiques à ceux prévus par l'article 34 de la directive NIS 2. La commission peut également décider de publier la sanction selon des modalités qu'elle précise, les frais étant supportés par la personne sanctionnée (art. L. 1332-18 nouveau).

Les administrations de l'État et ses établissements publics administratifs, les collectivités territoriales et leurs groupements ou établissements publics administratifs ne peuvent être sanctionnés par une amende administrative (**alinéa 91**).

m. Articles L. 1332-20 à L. 1332-22 (nouveaux) : marchés publics et contrats de concession

Les alinéas 100 à 106 introduisent les articles L. 1332-20 à 22 du code de la défense qui autorisent les OIV à recourir aux régimes dérogatoires des marchés publics et des contrats de concession. Ces dispositifs sont prévus dans le code de la commande publique respectivement au titre II du livre V de la deuxième partie du code et au titre II du livre II de la troisième partie du code. Ces régimes permettent de se soustraire à l'obligation de mise en concurrence et de publicité.

L'objectif de cette disposition est de se prémunir du risque d'ingérence étrangère, en évitant qu'un acteur hostile se porte candidat à des marchés publics ou des contrats de concessions et, le cas échéant, remporte le contrat. Actuellement, le code de la commande publique soumet au seul titre II du livre V de la deuxième partie les marchés publics qui exigent le secret ou dont l'exécution doit s'accompagner de mesures particulières de sécurité. Le présent projet de loi précise les marchés publics et les concessions des OIV qui pourront recourir à un tel dispositif. Le SGDSN a indiqué à l'occasion de son audition que le dispositif restera exceptionnel.

Deux conditions cumulatives doivent être réunies : (i) concerner des marchés ou des contrats de concessions 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 ; (ii) la protection ou la prévention du détournement d'usage ne peut être garantie par d'autres moyens.

Afin de garantir la conformité au droit de l'Union, les OIV devront informer l'autorité administrative qu'ils mettent en œuvre ces mesures, selon des modalités prévues par voie réglementaire (**alinéa 106**).

Si ces dispositions ne sont pas issues de la directive REC, elles s'inscrivent dans le cadre normatif européen, en particulier l'article 14 de la directive 2014/24 [(1)] et l'article 24 de la directive 2014/25 [(2)] sur les marchés publics qui prévoient une exclusion de l'application des règles de passation pour des raisons de sécurité.

3. Les modifications apportées par le Sénat

a. Articles L. 1332-1 : définitions

Un amendement porté par M. Vallet, du groupe socialiste, a été adopté en commission spéciale pour préciser la notion d'activité d'importance vitale, à l'alinéa 7. Toutefois un amendement du gouvernement en séance publique, soutenu par la commission, a rétabli la rédaction initiale, pour ne pas restreindre la notion.

En commission spéciale, les rapporteurs ont ajouté les définitions d'incident et de résilience à l'article L. 1332-1, absentes du projet de loi initial :

– incident (**alinéa 12**) : « *un événement qui perturbe ou est susceptible de perturber de manière importante l'exercice d'une activité d'importance vitale* » ;

– résilience (**alinéa 13**) : « *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* ».

Les définitions s'inspirent de celles présentes dans la directive REC à l'article 2 mais renvoient à la notion d'activité d'importance vitale à la place de celle d'entité critique, pour tenir compte de la nomenclature en droit national.

---

(1)Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE.

(2)Directive 2014/25/UE du Parlement européen et du Conseil du 26 février 2014 relative à la passation de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux et abrogeant la directive 2004/17/CE.

Le gouvernement, en séance publique, a précisé la définition de résilience introduite en commission spéciale comme « *la capacité d'un opérateur à prévenir à se protéger et à résister contre tout type d'incident afin d'assurer la continuité de la ou des activités d'importance vitale qu'il exerce.* » L'amendement du gouvernement, soutenu par la commission, dispose ainsi que la finalité de la résilience est de pouvoir résister aux attaques pour poursuivre les activités d'importance vitale.

b. Article L. 1332-3 (modifié) : évaluation des risques, mesures de résilience et plan de résilience opérateur des OIV

Un amendement porté par M. Vallet, du groupe socialiste, a été adopté en commission spéciale pour préciser la notion de risques à l'**alinéa 22** comme les risques : *« naturels ou d'origine humaine, accidentels ou intentionnels, y compris à caractère terroristes et ceux qui revêtent un caractère transsectoriel ou transfrontière ».* Toutefois un amendement du gouvernement en séance publique, soutenu par la commission, a rétabli la rédaction initiale, pour conserver l'approche la plus large possible des risques devant être analysés par les opérateurs.

La commission spéciale a adopté un amendement, porté par les rapporteurs, qui précise que l'astreinte pécuniaire, prévue à l'article L. 1332-3 du projet de loi en cas de refus des opérateurs d'élaborer un PRO, ne peut être imposée qu'à compter de l'expiration du délai imparti par la mise en demeure.

c. Article L. 1332-4 (modifié) : analyse des dépendances

La commission spéciale a adopté un amendement, porté par les rapporteurs, qui précise que l'analyse des dépendances à l'égard de tiers ne se limite pas à leur chaîne d'approvisionnement mais inclue également leurs sous-traitants. Toutefois, alors que la directive REC ne prévoit pas de prendre en compte les sous-traitants, un amendement du gouvernement en séance publique a supprimé cette mention. Les rapporteurs ne s'y sont pas opposés (sagesse).

d. Article L. 1332-5 (modifié) : établissement d'un plan particulier de résilience

La commission spéciale a adopté un amendement, porté par les rapporteurs, qui précise que l'astreinte pécuniaire, prévue à l'article L. 1332-5 du projet de loi en cas de refus des opérateurs d'élaborer un PPR, ne peut être imposée qu'à compter de l'expiration du délai imparti par la mise en demeure.

e. Article L. 1332-7 (nouveau) : notification des incidents

Alors que le projet de loi initial laissait à un décret en Conseil d'État la fixation du délai de notification d'un incident par l'opérateur à l'autorité administrative, un amendement adopté en commission spéciale et porté par les rapporteurs a précisé que ce délai est au plus tard de 24 heures après que l'opérateur a pris connaissance d'un incident. Ce délai est prévu par la directive REC.

f. Article L. 1332-9 (nouveau) : missions de conseil de la Commission européenne

Un amendement porté par M. Vallet et adopté en commission spéciale a précisé que la demande de mission de conseil ne pouvait se faire que sur demande motivée de la Commission européenne ou d'un ou plusieurs États membres dans lesquels l'opérateur exerce sa mission.

Si le projet de loi initial prévoyait que les missions de conseil ne peuvent être effectuées qu'avec l'accord des autorités étatiques compétentes, l'amendement a permis de préciser que cette inspection exige également au préalable la présentation d'une demande motivée de la Commission européenne ou d'un ou de plusieurs des États membres auxquels ou dans lesquels le service essentiel est fourni, conformément à l'article 18 de la directive REC.

g. Article L. 1332-11 (nouveau) : systèmes d'information d'importance vitale

Un amendement des rapporteurs en commission spéciale a étendu la capacité 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.

h. Article L. 1332-15 à L. 1332-19 (nouveaux) : commission des sanctions

La commission spéciale, à la suite d'un amendement des rapporteurs, a modifié la nomination des trois personnalités qualifiées à la commission des sanctions. Alors que le projet de loi initial prévoyait que les trois personnalités étaient nommées par le premier ministre, elles seront nommées par le premier ministre, le président de l'Assemblée nationale et le président du Sénat.

4. La position de la commission

La commission a adopté l'article 1er modifié par plusieurs amendements. Elle a adopté plusieurs amendements rédactionnels portés par la rapporteure Catherine Hervieu.

a. Articles L. 1332-1 et L. 1332-2 (modifiés) : définitions

La rapporteure Catherine Hervieu ainsi que le groupe Écologiste et Social (EcoS) ont proposé d'ajouter la préservation de l'environnement à la définition des activités d'importance vitale (**alinéa 7**). L'environnement n'est pas mentionné dans la définition actuelle des activités d'importance vitale, alors même que la plupart des secteurs d'application de la directive REC sont directement liés à sa préservation (énergie, transports, eau potable, denrées alimentaires). À ce titre, le point 478 de la revue nationale stratégique 2025, qui concerne la résilience des infrastructures critiques, indique spécifiquement que le risque environnemental

devrait être mieux intégré au dispositif. Toutefois, la Commission a rejeté cet amendement, avec un avis défavorable du rapporteur général Éric Bothorel.

Un amendement, porté par le rapporteur général Éric Bothorel et la rapporteure Catherine Hervieu, a permis de mettre en cohérence la notion d'infrastructure critique utilisée en droit européen avec celle de point d'importance vitale utilisée en droit national (**alinéa 9**).

La directive REC adopte une définition de la notion d'infrastructure critique plus large que celle couvrant le périmètre actuel de la notion de PIV, cette dernière étant déjà bien appréhendée par les opérateurs. Par conséquent, le projet de loi avait fait le choix de conserver le périmètre actuel des points d'importance vitale, et de concevoir ces derniers comme une catégorie spécifique d'infrastructure critique au sens de la directive, par l'emploi de l'adverbe « notamment ». Toutefois, la multiplication des textes européens faisant référence à la notion d'infrastructure critique rend de moins en moins pertinente la distinction [(1)].

Pour des raisons de cohérence entre le droit européen et le droit interne, l'amendement lève cette distinction. Il supprime le mot « notamment » pour assurer une identité entre, d'une part, les points d'importance vitale et les systèmes d'information d'importance vitale et, d'autre part, les infrastructures critiques.

b. Article L. 1332-4 (modifié) : analyse des dépendances

La Commission a adopté un amendement, porté par la rapporteure Catherine Hervieu, qui étend l'analyse des dépendances aux sous-traitants, selon un délai fixé par voie réglementaire (**alinéa 32**). Conformément aux dispositions prévues par la directive REC, l'interdépendance croissante de l'économie nécessite de la part des opérateurs d'importance vitale une analyse détaillée des vulnérabilités de leur chaîne d'approvisionnement. Or, cette analyse n'est pas complète sans prendre en compte les sous-traitants, dans une démarche analogue à celle prévue par la directive de 2024 sur le devoir de vigilance [(2)]. Afin d'éviter de surcharger les opérateurs, l'amendement précise que cette analyse sera réalisée selon un délai supplémentaire aux 9 mois prévus pour l'analyse des dépendances par la directive REC. Ce délai sera fixé par voie réglementaire.

La commission a également adopté un amendement du président Philippe Latombe qui étend l'analyse des dépendances aux vulnérabilités envers les fournisseurs de solutions logicielles (**alinéa 32**). Cet amendement précise que

---

(1) Cf. Recommandation du Conseil du 25 juin 2024 relative à un schéma directeur visant à coordonner au niveau de l'Union la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable ; Règlement (UE) 2024/1309 du Parlement européen et du Conseil du 29 avril 2024 relatif à des mesures visant à réduire le coût du déploiement de réseaux gigabit de communications électroniques, modifiant le règlement (UE) 2015/2120 et abrogeant la directive 2014/61/UE (règlement sur les infrastructures gigabit) ; Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) ; Conclusions du Conseil portant sur la révision de la stratégie de sureté maritime de l'UE (SSMUE) et son plan d'action ; Recommandation (UE) 2024/779 de la Commission du 26 février 2024 pour des infrastructures de câbles sous-marins sûres et résilientes.

(2) Directive 2024/1760 du Parlement européen et du Conseil du 13 juin 2024 sur le devoir de vigilance des entreprises en matière de durabilité et modifiant la directive (UE) 2019/1937 et le règlement (UE) 2023/2859.

l'analyse menée par les opérateurs évalue spécifiquement les dépendances envers les solutions logicielles et matérielles propriétaires.

c. Article L. 1332-5 (modifié) : établissement d'un plan particulier de résilience

La commission spéciale a adopté un amendement, porté par le rapporteur général Éric Bothorel, le président Philippe Latombe et la vice-présidente Virginie Duby-Muller, pour distinguer, dans le plan particulier de résilience, les dispositifs et les dispositions de résilience (**alinéa 35**). Le plan particulier de résilience, établi par l'opérateur pour chaque PIV, devra préciser les mesures qui relèvent d'équipements spécifiques et celles qui dépendent de procédures à mettre en œuvre.

d. Article L. 1332-6 (modifié) : enquêtes administratives de sécurité

La commission spéciale a adopté un amendement porté par le rapporteur général Éric Bothorel, M. Édouard Bénard et les groupes La France Insoumise (LFI) et Écologiste et Social, qui ajoute un avis de la CNIL sur le décret en Conseil d'État précisant les modalités de l'avis de l'autorité administrative sur une autorisation d'accès à un point d'importance vitale (**alinéa 40**). L'avis de la CNIL permettra d'éclairer le gouvernement sur les conditions dans lesquelles doivent s'effectuer les enquêtes administratives de sécurité en matière de protection de données privées et d'accès à des informations personnelles.

e. Article L. 1332-11 (nouveau) : systèmes d'information d'importance vitale

Un amendement du rapporteur général Éric Bothorel a clarifié les obligations des OIV à l'égard de la directive NIS 2, transposée par le titre II du présent projet de loi (**alinéa 60**).

D'une part, l'amendement soumet les OIV à l'obligation de notification des incidents à leurs destinataires de services, prévue à l'article 17 du présent projet de loi et issue de la directive NIS 2.

D'autre part, l'amendement clarifie les obligations applicables aux OIV qui n'entrent pas dans le champ d'application de NIS 2 avec celles qui leurs sont applicables en vertu d'un acte juridique sectoriel de l'Union européenne. En effet, il existe des OIV qui ne sont pas considérés comme des entités essentielles ou importantes au sens de la directive NIS 2. En revanche, ils peuvent entrer dans le champ d'application de règlementations sectorielles de l'Union relatives à la sécurité des réseaux et des systèmes d'informations. Dès lors, cet amendement précise que les opérateurs ne seront pas tenus de mettre en œuvre les obligations prévues aux articles 14 et 15 du projet de loi, afin de ne pas multiplier les exigences de sécurité qui auraient une même finalité et un effet équivalent.

f. Article L. 1332-15 à L. 1332-19 (nouveaux) : commission des sanctions

La Commission a adopté un amendement, porté par le rapporteur général Éric Bothorel, qui prévoit la nomination des personnalités qualifiées de la

commission des sanctions par le premier ministre plutôt que par le premier ministre, le président de l'Assemblée nationale et le président du Sénat (**alinéa 83**). Cet amendement a rétabli le dispositif du projet de loi initial, contre l'avis de la rapporteure Catherine Hervieu, qui considérait utile que le parlement intervienne dans la nomination des membres de la commission, en particulier pour des personnalités qualifiées.

Un amendement, porté par le rapporteur général Éric Bothorel, le vice-président Laurent Mazaury, la rapporteure Catherine Hervieu et le groupe LFI a consacré le principe du contradictoire devant la commission des sanctions (**alinéa 87**).

Un amendement porté par la rapporteure Catherine Hervieu a supprimé la possibilité de renouveler le mandat des membres de la commission des sanctions (**alinéa 90**). Le mandat unique, plutôt que renouvelable une fois, permettra de garantir le caractère désintéressé et impartial des décisions prises par la commission. Néanmoins, en raison de l'adoption d'un amendement du rapporteur général Éric Bothorel, le mandat unique ne sera pas applicable aux personnalités qualifiées de la commission des sanctions, dont la durée de mandat n'est plus spécifiée dans le texte adopté par la Commission. Un amendement sera porté en séance par la rapporteure Catherine Hervieu pour appliquer un mandat non renouvelable à l'ensemble des membres de la commission des sanctions.

*

* *

CHAPITRE II
Dispositions diverses

Article 2

(art. L. 1331-1, L. 2113-2, L. 2151-1, L. 2151-4, L. 2171-6, L. 2321-2-1, L. 2321-3 et L. 4231-6 du code de la défense ; art. 226-3 du code pénal ; art. L. 33-1 et L. 33-14 du code des postes et des télécommunications électroniques ; art. L. 1333-9 du code de la santé publique ; art. L. 223-2 et 223-8 du code de la sécurité intérieure ; art. 15 de la loi n° 2006-961 du 1er août 2006 relative aux droits d'auteur et aux droits voisins)

Actualisation de références législatives

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article procède à des actualisations législatives pour tirer les conséquences du dispositif introduit à l'article 1er du présent projet de loi.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

- **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. Le dispositif proposé : une actualisation de références législatives qui tire les conséquences des modifications apportées par l'article 1er

L'article 2 actualise plusieurs références législatives afin de prendre en compte l'article 1er du présent projet de loi. Il actualise le code de la défense (**I**), le code pénal (**II**), le code des postes et des communications électroniques (**III**), le code de la santé publique (**IV**), le code la sécurité intérieure (**V**) et la loi n° 2006-961 du 1er août 2006 relative aux droits d'auteur et aux droits voisins (**VI**).

S'agissant du code de la défense (**I**) :

– à l'article L. 1333-1, qui concerne la protection des sites nucléaires, la référence aux « *établissements, installations et ouvrages relevant de l'article L. 1332-1* » est remplacée par la référence à « *certaines infrastructures des opérateurs d'importance vitale mentionnés au 1° du I de l'article L. 1332-2* », c'est-à-dire des opérateurs exerçant une activité d'importance vitale autre que sur une installation nucléaire de base ou classée protection de l'environnement (**alinéa 2**) ;

– à l'article L. 2113-1, qui concerne la collaboration de ressortissants étrangers en temps de guerre, la référence aux *« installations ou aux ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 »* est remplacée par la référence aux « *opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 3**) ;

– à l'article L. 2151-1, qui concerne l'applicabilité du service de sécurité nationale au personnel visé par un plan de continuité d'activité, est introduite la référence aux *« documents de planification des opérateurs désignés au titre de l'article L. 1332-1 visant à garantir la continuité de leur activité »* (**alinéa 4**) ;

– à l'article L. 2151-4, qui renvoie à l'article ci-dessus, la mention *« des plans de continuité ou de rétablissement d'activité »* est supprimée (**alinéa 5**) ;

– au deuxième alinéa de l'article L. 2171-6, qui concerne la dispense de mobilisation de la réserve de sécurité nationale pour les agents exerçant dans un opérateur d'importance vitale, la référence aux opérateurs *« publics et privés ou des gestionnaires d'établissements désignés par l'autorité administrative conformément aux articles L. 1332-1 et L. 1332-2 »* est remplacée par la référence aux opérateurs « *d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 6**) ;

– aux premier et quatrième alinéas de l'article L. 2321-2-1, qui concerne la sécurité des systèmes d'information des opérateurs, la référence aux opérateurs mentionnés *« aux articles L. 1332-1 et L. 1332-2 »* est remplacée par la référence aux opérateurs *« d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 7**) ;

– à l'article L. 2321-3, qui concerne la sécurité des systèmes d'information des opérateurs, les références aux opérateurs *« mentionnés aux articles L. 1332-1 et L. 1332-2 »* sont remplacées par les références aux opérateurs *« d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéas 9 et 10**) ;

– à l'article L. 4231-6, qui concerne la dispense de disponibilité pour la réserve pour les agents exerçant dans un opérateur d'importance vitale, la référence aux opérateurs *« publics et privé ou des gestionnaires d'établissements désignés par l'autorité administrative conformément aux articles L. 1332-1 et L. 1332-2 »* est remplacée par la référence aux opérateurs « *d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 11**).

S'agissant du code pénal (**II**), à l'article 226-3, la référence aux opérateurs *« mentionnés à l'article L. 1332-1 »* est remplacée par la référence aux opérateurs *« d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 12**).

S'agissant du code des postes et des communications électroniques (**III**) :

– la référence aux opérateurs *« mentionnés aux articles L. 1332-1 et L. 1332-2 »* est remplacée par la référence aux opérateurs *« d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 14**) ;

– la référence aux opérateurs *« mentionnés à l'article L. 1332-1 »* est remplacée par la référence aux opérateurs « *d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 »,* c'est-à-dire des opérateurs exerçant une activité d'importance vitale autre que sur une installation nucléaire de base ou classée protection de l'environnement (**alinéa 15**).

S'agissant du code de la santé publique (**IV**), les références à « *certains établissements, installations et ouvrages relevant de l'article L. 1332-1* » sont remplacées par les références à « *certaines infrastructures des opérateurs d'importance vitale mentionnés au 1° du I de l'article L. 1332-2* », c'est-à-dire des opérateurs exerçant une activité d'importance vitale autre que sur une installation nucléaire de base ou classée protection de l'environnement (**alinéa 16**).

S'agissant du code de la sécurité intérieure (**V**), les références aux opérateurs « *exploitant des établissements, installations et ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 »* sont remplacées par les références aux *« opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 »*, c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéas 18 et 19**).

S'agissant de la loi n° 2006-961 du 1er août 2006 relative aux droits d'auteur et aux droits voisins (**VI**), la référence aux opérateurs *« publics ou privés gérant des installations d'importance vitale au sens des articles L. 1332-1 à L. 1332-7 »* est remplacée par la référence aux opérateurs « *d'importance vitale mentionnés au I de l'article L. 1332-2 »,* c'est-à-dire les opérateurs exerçant une activité d'importance vitale (**alinéa 20**).

2. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

3. La position de la commission

La commission spéciale a adopté l'article 2 modifié par un amendement rédactionnel porté par la rapporteure Catherine Hervieu.

*

* *

Article 3

(art. L. 6221-2, L. 6222-1, L. 6242-2 et L. 6312-3 [nouveaux] du code de la défense ; art. 711-1 du code pénal ; art. L. 33-1, L. 33-15 et L. 34-14 du code des postes et des communications ; art. L. 285-1, L. 286-1, L. 287-1 et L. 288-1 du code de la sécurité intérieure)

Dispositions relatives à l'outre-mer

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit les modalités d'application du dispositif introduit à l'article 1er en outre-mer. Le dispositif s'appliquera sur l'ensemble du territoire national, qu'il s'agisse des collectivités d'outre-mer régies par le principe d'identité législative ou de spécialité législative.

Toutefois, les dispositions spécifiques aux entités critiques d'importance européenne particulière ne seront pas applicables dans les pays et territoires d'outre-mer au sens du droit de l'Union : la Polynésie française, Wallis-et-Futuna, la Nouvelle-Calédonie, les Terres australes et antarctiques françaises (TAAF), Saint-Pierre-et-Miquelon et Saint-Barthélemy.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié au Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. Le dispositif proposé : une application du dispositif de SAIV sur l'ensemble du territoire

Conformément à l'article L. 1 du code de la défense, les dispositions du code de la défense sont applicables sur tout le territoire. À ce titre, le projet de loi

est applicable de plein droit aux collectivités d'outre-mer, de la même manière que le dispositif de SAIV actuel. Il s'agit des collectivités relevant à la fois du principe de l'identité législative – la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon – et du principe de spécialité législative – la Polynésie française, Wallis-et-Futuna, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises (TAAF).

Toutefois, le droit de l'Union distingue les régions ultrapériphériques (RUP), où le droit de l'Union est pleinement applicable, et les pays et territoires d'outre-mer (PTOM) qui ne sont pas intégrés à l'Union européenne. Les PTOM français sont les collectivités d'outre-mer régies par le principe de spécialité législative auxquelles s'ajoutent les collectivités de Saint-Pierre-et-Miquelon et Saint-Barthélemy.

Dès lors, la transposition de la directive REC issue de l'article 1er du présent projet de loi ne s'applique aux PTOM qu'en cas d'adaptation spécifique. L'article 3 adapte donc les dispositions du projet de loi aux PTOM pour assurer une application du dispositif de SAIV, en dehors des dispositions concernant les entités critiques d'importance européenne particulière (sous-section 2 de la section 1 du chapitre II du titre III du livre III du code de la défense, introduite par le présent projet de loi).

Le **I** du présent article est consacré aux adaptations du code de la défense.

Les **alinéas 2 et 3** créent un article L. 6221-2 au sein du code de la défense qui établit un principe de substitution automatique des références à des dispositions inapplicables à Saint-Barthélemy par des références à des dispositions applicables localement. La disposition reprend l'article R*. 6311-1 du code de la défense qui prévoit un tel dispositif pour Wallis-et-Futuna, la Polynésie française, la Nouvelle-Calédonie et les TAAF. Cette disposition garantit l'application du dispositif de SAIV aux pays et territoires d'outre-mer au sens du droit de l'Union.

Les **alinéas 4 à 9** précisent que les dispositions concernant les entités critiques d'importance européenne particulière ne sont pas applicables aux PTOM, à savoir Saint-Barthélemy (art. L. 6222-1 nouveau), Saint-Pierre-et-Miquelon (art. L. 6242-2 nouveau), Wallis-et-Futuna, la Polynésie française, la Nouvelle-Calédonie et les TAAF (art. L. 6312-3 nouveau).

Le **II** du présent article introduit un article 711-1 dans le code pénal pour préciser que les dispositions des livres Ier à V du code pénal sont applicables, dans leur rédaction résultant du présent projet de loi, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna (**alinéa 11**).

Le **III** du présent article modifie le code des postes et des communications électroniques pour faire référence à la présente loi aux articles L. 33-1, L. 33-15 et L. 34-14 (**alinéas 13 à 15**).

Le **IV** du présent article modifie le code de la sécurité intérieure pour faire référence à la présente loi aux articles L. 285-1, L. 286-1, L. 287-1 et L. 288-1 (**alinéa 16**).

2. Les modifications apportées

Le Sénat n'a pas modifié cet article.

3. La position de la commission

La commission spéciale a adopté l'article 3 modifié par un amendement rédactionnel de la rapporteure Catherine Hervieu, qui actualise les références législatives du code de la sécurité intérieure devant être modifiées par une référence à la présente loi.

*

* *

CHAPITRE III
Dispositions transitoires

Article 4
Modalités d'entrée en vigueur du titre I[er]

Adopté par la Commission

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit les modalités d'entrée en vigueur des dispositions prévues au titre I[er].

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

La commission spéciale du Sénat a précisé que l'entrée en vigueur du titre I[er] serait fixée à une date précisée par un décret en Conseil d'État, au plus tard un an après la promulgation du présent projet de loi.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. Le dispositif proposé : modalités d'entrée en vigueur des dispositions du titre Ier

L'article 4 fixe les modalités d'entrée en vigueur des dispositions prévues au titre Ier du présent projet de loi.

Le texte initial ne prévoyait pas de date d'entrée en vigueur du titre Ier. En l'absence de disposition spécifique, le titre Ier serait donc entré en vigueur au lendemain de la publication au *Journal officiel* du présent projet de loi, conformément aux règles fixées à l'article 1er du code civil. Néanmoins, la transposition de la directive REC en droit interne, prévue par le titre Ier du présent projet de loi, devait être réalisée au plus tard le 17 octobre 2024.

L'**alinéa 2** dispose que les opérateurs d'importance vitale désignés avant la date d'entrée en vigueur de la présente loi le resteront à l'entrée en vigueur de la loi et seront donc soumis automatiquement aux nouvelles obligations. À ce titre, ils seront soumis aux délais impartis suivants :

– neuf mois pour réaliser l'analyse des risques de toute nature prévue au premier alinéa de l'article L. 1332-3 ;

– dix mois pour réaliser le plan de résilience opérateur mentionné au quatrième alinéa de l'article L. 1332-3 ;

– neuf mois pour réaliser l'analyse des dépendances mentionnée à l'article L. 1332-4.

L'**alinéa 3** précise que les OIV désignés avant la date d'entrée en vigueur de la présente loi resteront soumis aux obligations applicables avant l'entrée en vigueur de la présente loi, jusqu'à l'accomplissement de leurs nouvelles obligations. L'objet de cet alinéa est d'éviter tout vide juridique dans la transition entre l'ancien et le nouveau dispositif de sécurité des activités d'importance vitale.

2. Les modifications apportées par le Sénat

À la suite d'un amendement déposé par les rapporteurs en commission, le **premier alinéa** de l'article 4 précise que le présent titre entrera en vigueur à une date fixée par décret en Conseil d'État, au plus tard un an après la promulgation de la présente loi. Ce délai vise à laisser le temps aux opérateurs de se conformer aux nouvelles obligations, en attendant la publication des actes d'application.

3. La position de la commission

La commission spéciale a adopté l'article 4 sans modification.

*

* *

TITRE II
CYBERSÉCURITÉ

CHAPITRE IER
De l'autorité nationale de sécurité des systèmes d'information

Adopté par la Commission avec modifications

Article 5
Missions et compétences de l'autorité nationale de sécurité des systèmes d'information (ANSSI)

➢ **Résumé du dispositif et effets principaux**

Cet article désigne l'ANSSI comme autorité compétente à l'échelle nationale en matière de cybersécurité, en plus de sa compétence initiale antérieure dans le domaine de la cyberdéfense.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté deux amendements : un amendement désignant explicitement l'ANSSI comme autorité nationale compétente et un amendement précisant que les missions de l'ANSSI « *comprennent notamment l'accompagnement et le soutien au développement de la filière cybersécurité en coordination avec les ministères compétents* ».

➢ **Modifications apportées par la commission**

La commission a adopté un amendement rédactionnel ainsi qu'un amendement complétant les missions de l'ANSSI en y incluant la promotion de la cyberprotection et de la cyberhygiène et de l'éducation aux bonnes pratiques numériques.

1. L'état du droit

Les compétences du premier ministre en matière de sécurité des systèmes d'information sont encadrées par le code de la défense. L'article L. 2321-1 dispose ainsi que le premier ministre « *définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information* » par l'intermédiaire de « *l'autorité nationale de sécurité des systèmes d'information*

qui assure la fonction d'autorité nationale de défense des systèmes d'information », qui, en l'espèce, correspond à l'ANSSI (article R. 2321-1).

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 (directive SRI 2), dite directive NIS 2, prévoit que « *chaque membre désigne ou établit une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de supervision* ».

2. Le dispositif proposé

L'article 5 du projet de loi prévoit, en conséquence, que l'ANSSI, unique autorité nationale compétente en matière de sécurité des systèmes d'information, assure les missions prévues par l'article 8 de la directive NIS 2. Ainsi, le **premier alinéa** dispose que l'ANSSI est chargée « *de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le [titre 2] et de son contrôle* ».

Au regard de ce champ très vaste, le projet de loi fait le choix, que n'impose pas la directive, de confier à une autorité unique le soin de piloter et coordonner la mise en œuvre de la politique du gouvernement en matière de cybersécurité et, en particulier, d'assurer le contrôle des obligations mises à la charge des opérateurs. Cette autorité unique sera l'ANSSI, service rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN) et déjà chargé de la défense des systèmes d'information par l'article L. 2321-1 du code de la défense. Toutefois, dans la mesure où le projet de loi soumet à une partie des obligations qu'il prévoit en application de la directive NIS2 des services de l'État exerçant en matière de défense des activités appelant un traitement particulier, le Conseil d'État a proposé dans son avis d'ajouter au projet de loi une disposition permettant au premier ministre de désigner, pour ces activités, une autre autorité.

L'**alinéa 2** prévoit également 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. Cette disposition concerne principalement le commandement de la cyberdéfense du ministère des armées, qui exerce, par délégation, les missions et les compétences de l'ANSSI à l'échelle du ministère des armées.

Les missions de l'ANSSI et les conditions d'exercices au titre de cet article seront précisées par décret en Conseil d'État (**alinéa 3**).

3. Les modifications apportées par le Sénat

Le Sénat a apporté deux modifications à l'article 5.

D'une part, il a introduit une référence à l'article L. 2321-1 du code de la défense pour désigner clairement l'ANSSI comme autorité nationale compétente. Il s'agissait d'un amendement de précision des rapporteurs, MM. Michel Canévet, Patrick Chaize et Hugues Saury, adopté en commission.

D'autre part, et même si les missions de l'ANSSI seront précisées par décret, le Sénat a complété l'alinéa 3 de l'article en précisant que ces missions « *comprennent notamment l'accompagnement et le soutien au développement de la filière cybersécurité en coordination avec les ministères compétents* ». Cet ajout a été motivé par le souci d'accompagner l'ensemble des entités concernées par les dispositions du titre II du projet de loi (entreprises, collectivités territoriales…) compte tenu de l'ampleur de la transformation induite par lesdites dispositions. Cet amendement, à l'initiative de Mme Catherine Morin-Desailly, a été adopté en commission.

4. La position de la commission

La commission spéciale a adopté un amendement rédactionnel de la rapporteure Anne Le Hénanff ainsi qu'un amendement de M. René Pilato et plusieurs de ses collègues du groupe La France insoumise-Nouveau Front populaire qui complète l'alinéa 3 par les mots : « *ainsi que la promotion de la cyberprotection et de la cyberhygiène et de l'éducation aux bonnes pratiques numériques* ». L'objectif de cet amendement est de compléter les missions de l'ANSSI en y incluant que la promotion de la cyberprotection et de la cyberhygiène et de l'éducation aux bonnes pratiques numériques.

*

* *

Article 5 bis A (nouveau)

Inscription dans les plans communaux de sauvegarde du risque d'incident informatique ayant un impact important sur la fourniture des services à la population

Introduit par la Commission spéciale

➢ **Résumé du dispositif et effets principaux**

Cet article inscrit à l'article L. 731-3 du code de la sécurité intérieure l'obligation pour les plans communaux de sauvegarde d'inclure le risque d'incident informatique ayant un impact important sur la fourniture des services à la population.

➢ **Dernières modifications législatives intervenues**

(sans objet).

1. L'état du droit

L'article L. 731-3 du code de la sécurité intérieure décrit le contenu du plan communal de sauvegarde. Celui-ci prépare la réponse aux situations de crise et regroupe l'ensemble des documents de compétence communale contribuant à l'information préventive et à la protection de la population. Il détermine, en fonction des risques connus, les mesures immédiates de sauvegarde et de protection des personnes, fixe l'organisation nécessaire à la diffusion de l'alerte et des consignes de sécurité, recense les moyens disponibles et définit la mise en œuvre des mesures d'accompagnement et de soutien de la population.

La mise en place, l'évaluation régulière et les éventuelles révisions du plan communal de sauvegarde peuvent être assurées par un adjoint au maire ou un conseiller municipal chargé des questions de sécurité civile désigné par le maire ou, à défaut, par le correspondant incendie et secours.

Les plans communaux de sauvegarde sont obligatoires pour chaque commune. Par ailleurs, la mise en œuvre des mesures de sauvegarde relève de chaque maire sur le territoire de sa commune.

Les plans communaux de sauvegarde sont arrêtés par le maire et, à Paris, par le préfet de police. Tous les cinq ans au moins, leur mise en œuvre fait l'objet d'un exercice associant les communes et les services concourant à la sécurité civile. Dans la mesure du possible, cet exercice implique aussi la population.

2. Le dispositif introduit par la commission spéciale

Cet article additionnel a été introduit par un amendement du rapporteur général Éric Bothorel, prévoyant l'obligation pour les plans communaux de sauvegarde d'inclure le risque d'incident informatique ayant un impact important sur la fourniture des services à la population.

*

* *

Article 5 bis
Stratégie nationale en matière de cybersécurité

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit que le premier ministre élabore une stratégie nationale de cybersécurité, conformément aux stipulations de l'article 7 de la directive dite NIS 2.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a introduit cet article additionnel en commission pour transposer les stipulations de l'article 7 de la directive dite NIS 2.

En séance, trois amendements ont été adoptés pour préciser que la stratégie nationale en matière de cybersécurité devra, d'une part, fixer les orientations permettant une approche intégrée des enjeux de cybersécurité et de souveraineté numérique, d'autre part, faire état des modalités de soutien aux collectivités territoriales et à leurs groupements pour la mise en œuvre des dispositions du titre II, et enfin, permettre l'identification et le renforcement des compétences et formations nécessaires sur l'ensemble du territoire.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté de nombreux amendements.

Plusieurs amendements ont complété la stratégie nationale de cybersécurité par l'ajout de nouvelles thématiques telles que la notion d'autonomie stratégique, l'amélioration du niveau général de sensibilisation à la cybersécurité, l'éducation et la formation en matière de cybersécurité et de cyberdéfense ou encore la promotion de l'utilisation de logiciels libres.

Deux amendements ont porté plus spécifiquement sur la question des collectivités territoriales. Un amendement a prévu la création, dans le cadre de la stratégie nationale, d'un fonds de soutien spécifiquement destiné à accompagner certaines collectivités territoriales et leurs établissements publics. Un second amendement a précisé que la stratégie nationale devrait également prévoir une dimension relative à l'aménagement du territoire.

1. L'état du droit

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, dite directive NIS 2, stipule que « *chaque État membre adopte une stratégie nationale en matière de cybersécurité* ».

Or, si une stratégie nationale en matière de cybersécurité est en cours de finalisation sous l'égide du secrétariat général de la défense et de la sécurité nationale (SGDSN), celle-ci n'a toujours pas été rendue publie et aucune disposition législative n'en a fixé le cadre.

2. Le dispositif proposé

Le **premier alinéa** dispose que « *le Premier ministre élabore une stratégie nationale en matière de cybersécurité* », et ce dans le but « *de parvenir à un niveau élevé de cybersécurité et de le maintenir* ».

Les **alinéas 2 à 10** détaillent le contenu de cette stratégie. Celle-ci devra en particulier comprendre :

– les objectifs et priorités de la Nation en matière de cybersécurité, couvrant en particulier les secteurs mentionnés à l'article 7 ;

– une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité ;

– un cadre de gouvernance visant une coordination renforcée ;

– un inventaire des mesures garantissant le partage d'informations sur les risques, les menaces et les incidents en matière de cybersécurité ainsi que la préparation, la réaction et la récupération des services après incident ;

– les orientations permettant une approche intégrée des enjeux de cybersécurité et de souveraineté numérique ;

– un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des entreprises, des administrations publiques et des citoyens à la cybersécurité ;

– les modalités de soutien aux collectivités territoriales et à leurs groupements ;

– l'identification et le renforcement des compétences et des formations nécessaires sur l'ensemble du territoire ;

– et les indicateurs clés de performance aux fins de l'évaluation de la mise en œuvre de la stratégie nationale en matière de cybersécurité.

L'**alinéa 11** prévoit que cette stratégie devra, en vertu de cet article, être mise à jour « *au moins tous les trois ans* ». Elle fera l'objet, « *à compter de 2026 et tous les deux ans* », d'un rapport remis au Parlement relatif à sa mise en œuvre (**alinéa 12**).

3. Les modifications apportées par le Sénat

Cet article additionnel a été introduit en commission à l'initiative des rapporteurs du projet de loi, MM. Michel Canévet, Patrick Chaize et Hugues Saury.

En séance publique, trois amendements, à l'initiative des membres du groupe « Socialiste, Écologiste et Républicain », ont été adoptés pour préciser que la stratégie nationale en matière de cybersécurité devra fixer les orientations permettant une approche intégrée des enjeux de cybersécurité et de souveraineté numérique, faire état des modalités de soutien aux collectivités territoriales et à leurs groupements, et enfin, permettre l'identification et le renforcement des compétences et formations nécessaires sur l'ensemble du territoire.

4. La position de la commission

Outre quatorze amendements rédactionnels de la rapporteure Anne Le Hénanff, la commission spéciale a adopté neuf amendements sur cet article.

Trois amendements du président Philippe Latombe ont :

– intégré la notion d'autonomie stratégique dans les objectifs et priorités de la Nation dans le cadre de la stratégie nationale de cybersécurité ;

– inscrit dans la stratégie nationale la fixation des orientations visant à promouvoir l'utilisation de logiciels libres et des standards ouverts ;

– prévu dans la stratégie nationale la création d'un fonds de soutien spécifiquement destiné à accompagner les collectivités territoriales et les EPCI à fiscalité propre qualifiés d'entités importantes ou essentielles n'ayant pas bénéficié du « parcours de cybersécurité » du plan France Relance.

S'agissant du plan comprenant les mesures nécessaires pour améliorer le niveau général de sensibilisation des entreprises, des administrations publiques et des citoyens à la cybersécurité, un amendement du rapporteur général Éric Bothorel a précisé que le plan doit être mis en place annuellement dès 2026 et piloté par le dispositif national d'assistance aux victimes d'actes de cybermalveillance et un amendement de M. René Pilato et plusieurs de ses collègues du groupe LFI-NFP a précisé qu'il devrait se traduire notamment par la mise en place de politiques actives de cyberprotection, de cyberhygiène et d'éducation aux bonnes pratiques numériques.

Deux amendements de M. Vincent Thiébaut, M. Xavier Albertini, Mme Le Hénanff et Mme Laetitia Saint-Paul ont :

– précisé que les modalités de soutien aux collectivités territoriales et à leurs groupements seront notamment de nature financière ;

– inscrit dans la stratégie nationale des objectifs de promotion et de développement de l'éducation et de la formation en matière de cybersécurité, des initiatives de sensibilisation, et de recherche et développement en matière de cybersécurité ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'attention des citoyens, des parties prenantes et des entités.

Un amendement de M. René Pliato et de plusieurs de ses collègues du groupe LFI-NFP a inscrit dans la stratégie nationale une stratégie d'aménagement du territoire comprenant le maillage territorial des compétences en matière de cybersécurité, les établissements d'enseignement supérieur, les lycées professionnels et les organismes de formation continue, les dispositifs de soutien aux collectivités territoriales pour leur mise en conformité, leur sécurisation numérique et leur capacité de résilience, et des objectifs de réduction des inégalités territoriales d'accès aux métiers, aux formations et aux ressources en cybersécurité.

Un amendement de M. Arnaud Saint-Martin et de plusieurs de ses collègues du groupe LFI-NFPIa inscrit dans la stratégie nationale un objectif de renforcement de l'offre de formation publique dans les domaines de la cybersécurité et de la cyberdéfense.

*

* *

CHAPITRE II
De la cyber-résilience

Section 1
Définitions

Article 6
Définitions

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article définit les principales notions nécessaires pour la mise en œuvre du dispositif national de cybersécurité imposé par la directive dite NIS 2.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté plusieurs amendements en commission pour introduire les définitions des notions d'incident et de vulnérabilité telles qu'elles figurent dans la directive NIS 2 et un amendement en séance, pour préciser la notion de vulnérabilité telle qu'elle a été insérée en commission.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté des amendements à cet article visant en particulier à définir les notions d'« agent agissant pour le compte des bureaux d'enregistrement » et de « résilience ».

1. L'état du droit

L'article 6 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, dite directive NIS 2, liste les définitions des notions employées dans la directive. Il en comporte quarante et une.

Liste des notions employées à l'article 6 de la directive dite NIS 2

1) « réseau et système d'information »

2) «sécurité des réseaux et des systèmes d'information »

3) « cybersécurité »

4) « stratégie nationale en matière de cybersécurité »

5) « incident évité »

6) « incident »

7) « incident de cybersécurité majeur »

8) « traitement des incidents »

9) « risque »

10) « cybermenace »

11) « cybermenace importante »

12) « produit TIC »

13) « service TIC »

14) « processus TIC »

15) « vulnérabilité »

16) « norme »

17) « spécification technique »

18) « point d'échange internet »

19) « système de noms de domaine » ou « DNS »

20) « fournisseur de services DNS »

21) « registre de noms de domaine de premier niveau »

22) « entité fournissant des services d'enregistrement de noms de domaine »

23) « service numérique »

24) « service de confiance »

25) « prestataire de services de confiance »

26) « service de confiance qualifié »

27) « prestataire de services de confiance qualifié »

28) « place de marché en ligne »

29) « moteur de recherche en ligne »

30) « service d'informatique en nuage »

31) « service de centre de données »

32) « réseau de diffusion de contenu »

33) « plateforme de services de réseaux sociaux »

34) « représentant »

35) « entité de l'administration publique »

36) « réseau de communications électroniques public »

37) « service de communications électroniques »

38) « entité »

39) « fournisseur de services gérés »

40) « fournisseur de services de sécurité gérés »

41) « organisme de recherche »

2. Le dispositif proposé

L'article 6 du projet de loi se limitait initialement à la définition des notions suivantes :

– les bureaux d'enregistrement (**alinéa 2**) ;

– les offices d'enregistrement (**alinéa 3**) ;

– les prestataires de services de confiance (**alinéa 5**) ;

– les prestataires de services de confiance qualifiés (**alinéa 6**) ;

– les représentants (**alinéa 7**) ;

– les services de centre de données (**alinéa 8**) ;

– et les systèmes d'information (**alinéa 9**).

Par ailleurs, les notions retenues dans l'article 6 du projet de loi, y compris dans leurs formulations, ne reprennent pas exactement celles prévues à l'article 6 de la directive.

Par exemple, tandis que l'article 6 de la directive NIS 2 retient les notions d'entité fournissant des services d'enregistrement de noms de domaine d'une part, et de registre de noms de domaine de premier niveau d'autre part, l'article 6 du projet de loi distingue les bureaux d'enregistrement et les offices d'enregistrement.

Ce choix se justifie essentiellement par la nécessité d'adapter les dispositions du projet de loi aux spécificités nationales.

3. Les modifications apportées par le Sénat

Le Sénat a apporté plusieurs modifications à l'article 6.

Tout d'abord, il a ajouté des définitions qui ne figuraient pas dans la version initiale de l'article. En particulier, il a inscrit la définition de la notion d'incident (**alinéa 4**) en reprenant à l'identique celle prévue à l'article 6 de la directive NIS 2. Cet ajout a été effectué en commission à l'initiative des rapporteurs MM. Michel Canévet, Hugues Saury et Patrick Chaize.

Par ailleurs, il a ajouté la définition de la notion de vulnérabilité (**alinéa 10**), là encore en reprenant à l'identique la définition prévue à l'article 6 de la directive NIS 2. Cet ajout a également été effectué en commission à l'initiative des rapporteurs MM. Michel Canévet, Hugues Saury et Patrick Chaize.

Enfin, un amendement du gouvernement a été adopté en séance pour apporter une précision à la définition de la notion de vulnérabilité. Cet amendement visait à tenir compte du facteur humain susceptible de relever d'une vulnérabilité tout en le reliant directement à l'utilisation des produits et services des technologies de l'information et de la communication.

4. La position de la commission

Outre trois amendements rédactionnels de la rapporteure Anne Le Hénanff, la commission spéciale a adopté huit amendements à cet article :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff inscrivant la définition de la notion d'agent agissant pour le compte des bureaux d'enregistrement afin de clarifier les agents soumis aux dispositions du projet de loi. Cette définition vise notamment à dresser une liste non exhaustive de ces agents qui inclurait les revendeurs de noms de domaine ainsi que les fournisseurs de services d'anonymisation ou d'enregistrement fiduciaire comme le prévoit la directive ;

– deux amendements identiques de clarification du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff sur les office d'enregistrement, d'un

bureau d'enregistrement, d'un agent agissant pour le compte d'un bureau d'enregistrement afin d'harmoniser les définitions inscrites à l'alinéa 7 avec celles inscrites aux alinéas 1er et 2 de l'article ;

– un amendement de la rapporteure Anne Le Hénanff inscrivant la notion de résilience dans la liste des définitions de l'article, en reprenant celle inscrite dans le titre Ier du projet de loi ;

– trois amendements identiques du rapporteur général Éric Bothorel, de la rapporteure Anne Le Hénanff et de Mme Marina Ferrari visant à rapprocher la définition de la notion de vulnérabilité inscrite à l'article 3 du règlement dit CRA (Cyber Resilience Act), qui n'inclut pas de référence au facteur humain. Ainsi, la suppression des mots « *ou d'un utilisateur de ces derniers* » permet d'aligner la définition de la notion de vulnérabilité avec celle inscrite dans le droit européen.

*

* *

Section 2
Des exigences de sécurité des systèmes d'information

Article 7
Liste des secteurs d'activité hautement critiques et « critiques »

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

L'article 7 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement pour inscrire dans le projet de loi la liste des secteurs hautement critiques et critiques du point de vue de la cybersécurité.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté deux amendements rédactionnels.

1. L'état du droit

La 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, dite NIS 1, identifiait sept secteurs essentiels :

– l'énergie ;

– les transports ;

– les banques ;

– les infrastructures de marchés financiers ;

– la santé ;

– la fourniture et la distribution d'eau potable ;

– et les infrastructures numériques.

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, qui a transposé la directive NIS 1 en droit national a rajouté à cette liste sept secteurs supplémentaires :

– les assurances ;

– la restauration collective ;

– le traitement des eaux ;

– les organismes sociaux ;

– l'emploi et la formation professionnelle ;

– l'éducation.

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 (directive SRI 2), dite directive NIS 2, a considérablement étendu la liste des secteurs concernés, rebaptisés hautement critiques et « critiques », en intégrant de nouveaux secteurs d'activité.

La liste des dix-huit secteurs hautement critiques et critiques est établie respectivement par les annexes I et II de la directive. S'agissant des secteurs « hautement critiques », en plus des secteurs essentiels listés dans la directive NIS 1, figurent désormais les eaux usées, la gestion des services des technologies de

l'information et de la communication (TIC), l'administration publique (à l'exception de celles dont les activités portent sur la sécurité nationale, la sécurité publique, la défense ou l'application de la loi) et l'espace.

Par ailleurs, les secteurs critiques listés dans l'annexe II de la directive sont les 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, de produits informatiques, électroniques et optiques, d'équipements électriques, de machines et d'équipements, de véhicules et de matériels de transport ;

– les fournisseurs numériques ;

– et la recherche.

2. Le dispositif proposé

L'article 7 du projet de loi prévoyait initialement que la liste des secteurs hautement critiques et des secteurs critiques soit précisée par décret en Conseil d'État.

3. Les modifications apportées par le Sénat

Le Sénat a considérablement modifié l'article 7 du projet de loi en y inscrivant la liste des secteurs hautement critiques et des secteurs « critiques », estimant que le renvoi à un décret en Conseil d'État de la liste desdits secteurs n'était pas opportun. Cette modification a été apportée en commission à l'initiative des rapporteurs MM. Michel Canévet, Hugues Saury et Patrick Chaize. La commission spéciale a estimé qu'il n'était pas acceptable que des dispositions aussi importantes que les listes des secteurs hautement critiques et « critiques », qui figurent dans les annexes I et II de la directive, ne soient pas inscrites dans le projet de loi et soient renvoyées à un décret en Conseil d'État.

Le **I** (**alinéas 1er à 11**) définit désormais les secteurs hautement critiques :

– l'énergie ;

– les transports ;

– les banques ;

– les infrastructures des marchés financiers ;

– la santé ;

– l'eau potable ;

– les eaux usées ;

– l'infrastructure numérique ;

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

– et l'espace.

Le **II (alinéas 12 à 19)** définit quant à lui les secteurs critiques :

– les services postaux et d'expédition ;

– la gestion des déchets ;

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

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

– la fabrication de certains biens, équipements et produits ;

– les fournisseurs de certains services numériques ;

– et la recherche.

Toutefois, le **III** (**alinéa 20**) renvoie à un décret en Conseil d'État les modalités d'application de l'article ainsi que la liste des sous-secteurs et les entités relevant des secteurs hautement critiques et critiques. Ce choix est justifié par le souhait de laisser au gouvernement les marges de manœuvre nécessaires pour l'application de l'article, afin de tenir compte notamment du caractère fluctuant des périmètres ministériels qu'il ne conviendrait pas de figer au niveau de la loi.

4. La position de la commission

La commission spéciale a adopté deux amendements rédactionnels de la rapporteure Anne Le Hénanff.

*

* *

Article 8
Définition des entités essentielles

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article précise la liste des entités considérées comme essentielles du point de vue de la sécurité des systèmes d'information.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté quatre amendements en séance publique. Le premier amendement met en cohérence le projet de loi à la suite de l'amendement à l'article 7 listant les secteurs hautement critiques et critiques du point de vue de la cybersécurité et remplace, lorsque cela était nécessaire, le critère de l'appartenance à un secteur d'activité par celui de l'appartenance à un type d'entités.

En outre, trois amendements ont exclu du champ d'application de l'article les communautés d'agglomération ne comprenant pas au moins une commune d'une population supérieure à 30 000 habitants.

➢ **Modifications apportées par la commission**

Outre plusieurs amendements rédactionnels, la commission spéciale a adopté des amendements visant à :

– exempter les entités dont les activités relèvent de la sécurité nucléaire ;

– inclure les entreprises éditrices de logiciels dans la liste des entités essentielles ;

– inclure l'ensemble des communautés d'agglomération dans la catégorie des entités essentielles et non plus uniquement celles comprenant au moins une commune de plus de 30 000 habitants. Ce faisant, la commission spéciale est revenue à la rédaction initiale du texte ;

– inclure les établissements publics de santé et les établissements et services sociaux et médico-sociaux dans la liste des entités essentielles.

1. L'état du droit

L'article 3 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 (directive SRI 2), dite directive NIS 2, distingue deux catégories d'entités régulées : les entités essentielles et les entités importantes. La distinction entre les deux catégories s'établit selon leur degré de criticité, leur taille et, pour les entreprises, leur chiffre d'affaires.

2. Le dispositif proposé

L'article 8 transpose les articles 2 et 3 de la directive NIS 2 en établissant la liste des entités considérées comme essentielles en reprenant les critères fixés par ladite directive. Sont ainsi des entités essentielles :

– les entités appartenant à un secteur « hautement critique » dont les effectifs sont au moins de 250 personnes, dont le chiffre d'affaires annuel est supérieur à 50 millions d'euros ou dont le total du bilan annuel est supérieur à 43 millions d'euros (**alinéa 2**) ;

– les établissements publics à caractère industriel et commercial, à l'exception du Commissariat à l'énergie atomique et aux énergies alternatives pour ses seules activités dans le domaine de la défense, ainsi que les régies dotées de la seule autonomie financière chargées d'un service public industriel et commercial créées en application du 2° de l'article L. 2221-4 du code général des collectivités territoriales, relevant d'un type d'entités 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. Le critère d'emploi est calculé selon les modalités prévues au I de l'article L. 130-1 du code de la sécurité sociale, les critères financiers sont appréciés au niveau de la personne morale ou de la régie concernée (**alinéa 3**) ;

– 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 (**alinéa 4**) ;

– les prestataires de services de confiance qualifiés (**alinéa 5**) ;

– les offices d'enregistrement (**alinéa 6**) ;

– les fournisseurs de services de système de noms de domaine (**alinéa 7**) ;

– les administrations de l'État et leurs établissements publics administratifs (EPA), 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 ainsi que de leurs EPA qui exercent leurs activités dans les mêmes domaines ou qui sont désignés entité importante par arrêté du premier ministre. Le premier ministre désigne par arrêté 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, dans des conditions précisées par décret en Conseil d'État (**alinéas 8 et 9**) ;

– les régions, les départements, les communes d'une population supérieure à 30 000 habitants, leurs EPA dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques (**alinéa 10**) ;

– les centres de gestion mentionnés à l'article L. 452-1 du code général de la fonction publique (**alinéa 11**) ;

– les services départementaux d'incendie et de secours mentionnés à l'article L. 1424-1 du code général des collectivités territoriales (**alinéa 12**) ;

– les communautés urbaines, les communautés d'agglomération comprenant au moins une commune de plus de 30 000 habitants et les métropoles, leurs EPA dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques (**alinéa 13**) ;

– les syndicats mentionnés aux articles L. 5212-1, L. 5711-1 et L. 5721-2 du même code 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 (**alinéa 14**) ;

– les institutions et organismes interdépartementaux mentionnés à l'article L. 5421-1 dudit code dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques (**alinéa 15**) ;

– les autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif, mentionnés au 1° de l'article L. 100-3 du code des relations entre le public et l'administration, à compétence nationale, à l'exception de ceux qui sont désignés entité importante par arrêté du premier ministre. 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 (**alinéa 16**) ;

– les opérateurs d'importance vitale en tant qu'ils exercent une activité qualifiée de service essentiel en application du second alinéa du 1° du I de l'article L. 1332-2 du code de la défense (**alinéa 17**) ;

– les opérateurs de services essentiels désignés en application de l'article 5 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 avant l'entrée en vigueur de la présente loi (**alinéa 18**) ;

– et 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, qui remplissent l'un des critères mentionnés à l'article 10 de la présente loi (**alinéa 19**).

Il est à noter que le Conseil d'État relève dans son avis que le projet de loi mobilise dans un sens extensif les possibilités d'options offertes par la directive, notamment en incluant dans le champ du dispositif des collectivités territoriales autres que les régions, à savoir tous les départements ainsi que les communes et groupements de communes de plus de trente mille habitants, et, s'agissant d'un dispositif de défense et de sécurité nationale, en le rendant applicable à toutes les collectivités d'outre-mer, y compris celles auxquelles la directive n'est pas applicable. Il soumet en outre à un régime proche les services régaliens entendus au sens large. Ces choix, qui vont au-delà de ce qu'appelle strictement la transposition de la directive NIS 2, trouvent leur justification dans la volonté du gouvernement d'assurer en France un haut niveau de cybersécurité.

3. Les modifications apportées par le Sénat

Le Sénat a adopté quatre amendements en séance. Le premier amendement, à l'initiative du gouvernement, visait à mettre en cohérence le projet de loi à la suite de l'amendement à l'article 7 listant les secteurs hautement critiques et critiques du point de vue de la cybersécurité. Il visait également à remplacer, lorsque cela était nécessaire, le critère de l'appartenance à un secteur d'activité par celui de l'appartenance à un type d'entités.

En outre, trois amendements identiques, à l'initiative des groupes « Communiste Républicain Citoyen et Écologiste – Kanaky » et « Écologiste – Solidarité et Territoires » ainsi que des rapporteurs MM. Patrick Chaize, Hugues Saury et Michel Canévet, ont exclu du champ d'application de l'article les communautés d'agglomération comprenant au moins une commune d'une population supérieure à 30 000 habitants. Celles-ci ne sont donc pas considérées comme des entités essentielles. Ce choix a été motivé par la nécessité de ne pas faire peser une charge trop importante aux collectivités territoriales de petite taille. En pratique, selon les estimations du Sénat, 120 communautés d'agglomérations seraient, de ce fait, intégrées dans le périmètre des entités importantes.

4. La position de la commission

Outre trois amendements rédactionnels de la rapporteure thématique, la commission spéciale a adopté six amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff exemptant les entités dont les activités relèvent de la sécurité nucléaire, pour lesquelles la France souhaite pouvoir exercer pleinement et entièrement sa compétence exclusive en matière de sauvegarde de la sécurité et de la souveraineté nationales ;

– un amendement de Mme Véronique Riotton incluant les entreprises éditrices de logiciels dans la liste des entités essentielles ;

– un amendement de Mme Marina Ferrari incluant l'ensemble des communautés d'agglomération dans la catégorie des entités essentielles et non plus uniquement celles comprenant au moins une commune de plus de 30 000 habitants. Ce faisant, la commission spéciale est revenue à la rédaction initiale du texte ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff incluant les établissements publics de santé et les établissements et services sociaux et médico-sociaux dans la liste des entités essentielles.

*

* *

Article 9
Définition des entités importantes

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article définit la liste des entités considérées comme importantes du point de vue de la sécurité des systèmes d'information. Il s'agit des entités faisant l'objet de mesures de cybersécurité significatives mais qui sont toutefois moins exigeantes que celles qui s'appliquent aux entités essentielles listées à l'article 8 du projet de loi.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté deux amendements visant à mettre en cohérence le projet de loi à la suite de l'amendement à l'article 7 listant les secteurs hautement critiques et critiques du point de vue de la cybersécurité et à inclure dans la liste des communautés d'agglomération ne comprenant pas au moins une commune de 30 000 habitants dans la catégorie des entités importantes.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté plusieurs amendements visant en particulier à :

– exempter les entités dont les activités relèvent de la sécurité nucléaire ;

– inclure l'ensemble des communautés d'agglomération dans la catégorie des entités importantes et non plus uniquement celles comprenant au moins une commune de plus de 30 000 habitants. Ce faisant, la commission spéciale est revenue à la rédaction initiale du texte ;

– inclure les établissements publics de santé et les établissements et services sociaux et médico-sociaux dans la liste des entités importantes lorsque ceux-ci ne sont pas des entités essentielles.

1. L'état du droit

L'article 3 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, dite directive NIS 2, distingue deux catégories d'entités régulées : les entités essentielles et les entités importantes. La distinction entre les deux catégories s'établit selon leur degré de criticité, leur taille et, pour les entreprises, leur chiffre d'affaires.

Les critères de définition des entités importantes ne sont pas aussi explicites que ceux des entités essentielles dans la directive. En effet, les entités importantes sont les entités appartenant à un secteur hautement critique ou critique qui ne constituent pas des entités essentielles.

2. Le dispositif proposé

L'article 9 du projet de loi liste les entités importantes en creux par rapport à la liste des entités essentielles. Ainsi, sont des entités importantes :

– les entreprises appartenant à un secteur hautement critique ou critique 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 (**alinéa 2**) ;

– les opérateurs de communications électroniques qui ne sont pas des entités essentielles (**alinéa 3**) ;

– les prestataires de services de confiance qui ne sont pas des entités essentielles (**alinéa 4**) ;

– les communautés de communes et leurs établissements publics administratifs (EPA) dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques (**alinéa 5**) ;

– les établissements d'enseignement menant des activités de recherche qui ne sont pas des entités essentielles et qui, compte tenu du faible impact économique

et social de leur activité, ne sont pas soumis aux dispositions du projet de loi, dans des conditions fixées par décret en Conseil d'État (**alinéa 6**) ;

– les EPA expressément désignés par le premier ministre comme relevant de la catégorie des entités importantes en application de l'article 10 du projet de loi (**alinéa 7**) ;

– les autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif expressément désignés en tant qu'entités importantes par arrêté du premier ministre dans des conditions fixées par un décret en Conseil d'État (**alinéa 8**) ;

– et les établissements publics de coopération intercommunale (EPCI) et les régies dotées de la seule autonomie financière chargées d'un service public industriel et commercial appartenant à un secteur hautement critique ou critique qui emploient au moins 50 personnes ou dont le produit d'exploitation et le total du bilan annuel excèdent chacun 10 millions d'euros et qui ne sont pas des entités essentielles (**alinéa 9**).

3. Les modifications apportées par le Sénat

Le Sénat a adopté deux amendements en séance sur l'article 9. Le premier amendement, à l'initiative du gouvernement, met en cohérence le projet de loi à la suite de l'amendement à l'article 7 listant les secteurs hautement critiques et critiques du point de vue de la cybersécurité. Il visait également à remplacer, lorsque cela était nécessaire, le critère de l'appartenance à un secteur d'activité par celui de l'appartenance à un type d'entités.

Le second amendement, à l'initiative du rapporteur M. Patrick Chaize au nom de la commission spéciale, inclut à la liste des communautés d'agglomération ne comprenant pas au moins une commune de 30 000 habitants dans la catégorie des entités importantes. Cet amendement était en lien avec l'amendement déposé par les rapporteurs à l'article 8 du projet de loi excluant les communautés d'agglomération ne comprenant pas au moins une commune de 30 000 habitants de la liste des entités essentielles. L'objectif poursuivi était, dans un souci de proportionnalité, d'éviter d'imposer des obligations jugées excessives en matière de cybersécurité à des intercommunalités dont la taille ne le justifierait pas. D'après le Sénat, seront ainsi des entités importantes les 120 communautés d'agglomération qui ne comptent pas au moins une commune de plus de 30 000 habitants ainsi que les communautés de commune.

4. La position de la commission

Outre deux amendements rédactionnels de la rapporteure thématique, la commission a adopté cinq amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff exemptant les entités dont les activités relèvent de la sécurité nucléaire, pour lesquelles la France souhaite pouvoir exercer pleinement et entièrement sa compétence exclusive en matière de sauvegarde de la sécurité et de la souveraineté nationales ;

– un amendement de Mme Marina Ferrari incluant l'ensemble des communautés d'agglomération dans la catégorie des entités importantes et non plus uniquement celles comprenant au moins une commune de plus de 30 000 habitants. Ce faisant, la commission spéciale est revenue à la rédaction initiale du texte ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff incluant les établissements publics de santé et les établissements et services sociaux et médico-sociaux dans la liste des entités importantes lorsque ceux-ci ne sont pas des entités essentielles.

*

* *

Article 10

Autres entités susceptibles d'être désignées comme essentielles ou importantes par arrêté du premier ministre

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article transpose les stipulations de l'article 2 de la directive dite NIS 2 qui prévoit d'assujettir aux stipulations de ladite directive sans condition de taille des entités appartenant aux secteurs hautement critiques ou critiques, dès lors que la perturbation de leur service par une cyberattaque pourrait avoir un impact important pour le fonctionnement de la société, de secteurs économiques critiques, pour la sécurité publique, la sûreté publique ou encore la santé publique.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

Outre un amendement rédactionnel, la commission spéciale a adopté plusieurs amendements visant à :

– préciser que l'élaboration de la liste des entités essentielles et importantes doit être faite après avis des ministères compétents ;

– octroyer au premier ministre la possibilité d'exempter, par arrêté, certaines entités exerçant des missions régaliennes de certaines obligations prévues par les articles 14 et 17 du projet de loi.

1. L'état du droit

L'article 2 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, dite directive NIS 2, prévoit que la directive s'applique aux entités relevant d'un secteur d'activité hautement critique ou 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 (*b)* du 1.) ;

– une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique (c) du 1.) ;

– 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 (d) du 1.) ;

– 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 (e) du 1.).

2. Le dispositif proposé

L'article 10 prévoit qu'outre les entités mentionnées aux articles 8 et 9 du projet de loi, 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 au regard de plusieurs critères qui reprennent fidèlement la liste des critères fixés au 1. de l'article 2 de la directive NIS 2.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

Outre un amendement rédactionnel de la rapporteure Anne Le Hénanff, la commission spéciale a adopté trois amendements :

– un amendement du président Philippe Latombe précisant que l'élaboration de la liste des entités essentielles et des entités importantes doit être faite après avis des ministères compétents des secteurs d'activités mentionnés à l'article 7 du projet de loi ;

– deux amendements identiques du rapporteur général Éric Bothorel et de M. Vincent Thiébaut, M. Xavier Albertini et Mme Laetitia Saint-Paul octroyant au premier ministre la possibilité d'exempter, par arrêté, certaines entités exerçant des missions régaliennes (sécurité nationale, sécurité publique, défense, répression pénale…) de certaines obligations prévues par les articles 14 et 17 du projet de loi. L'objectif est de concilier l'application de la directive avec les impératifs de souveraineté et de sécurité nationale, en particulier s'agissant des obligations générales de notification ou de supervision.

*

* *

Article 11
Compétence et territorialité des dispositions du titre II

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

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

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

La commission n'a pas modifié cet article.

1. L'état du droit

Les règles de compétence des États membres pour l'application des dispositions 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, dite directive NIS 2, sont précisées à son article 26. Il s'agit avant tout de critères territoriaux.

Le paragraphe 1 de l'article 26 prévoit 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, à l'exception :

a) des fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils fournissent leurs services ;

b) des 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, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils ont leur établissement principal dans l'Union ;

c) et des entités de l'administration publique, qui sont considérées comme relevant de la compétence de l'État membre qui les a établies.

En outre, le paragraphe 2 de l'article 26 stipule que les entités visées au b) sont considérées avoir leur 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.

2. Le dispositif proposé

L'article 11 du projet de loi transpose fidèlement l'article 26 de la directive, en reprenant les critères fixés par celui-ci tout en les présentant de manière plus claire et plus détaillée. L'article distingue plusieurs catégories d'entités, auxquelles les critères de détermination de la compétence de l'État varient selon les cas.

Le **I** fixe les critères, alternatifs, permettant de déterminer le champ d'application territorial du projet de loi aux entités essentielles et importantes.

Le **II** définit les critères de territorialité spécifiques qui s'appliquent aux bureaux d'enregistrement.

Le **III** précise la manière dont la notion d'établissement principal doit être entendue. Cette notion est en effet utilisée à l'alinéa 5 s'agissant d'un certain nombre de fournisseurs de services et à l'alinéa 9 s'agissant des bureaux d'enregistrement. Il s'agit de la reprise fidèle du 2. de l'article 26 de la directive NIS 2, ce qui ne pose donc pas de difficulté.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale n'a pas modifié cet article.

*

* *

Article 12
Enregistrement des entités essentielles et importantes auprès de l'ANSSI

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit que l'ANSSI 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté des amendements à cet article visant à :

– inscrire dans la loi la nécessité de mettre à jour *a minima* tous les deux ans la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement concernés par les dispositions du titre II du projet de loi, conformément au 5. de l'article 3 de la directive NIS 2 ;

– prévoir que les informations transmises par les entités et les bureaux d'enregistrement à l'ANSSI doivent l'être « *dans le respect des modalités de*

chiffrement de bout en bout ainsi que de protection des données recueillies de l'effet des lois extraterritoriales ».

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant à :

– introduire la notion d'agents agissant pour le compte des bureaux d'enregistrement ;

– préciser que la liste des entités essentielles et importantes, des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers est communiquée après avis des ministères compétents ;

– préciser que le décret en Conseil d'État fixant les modalités d'application de l'article est pris après avis de la Commission nationale de l'informatique et des libertés (CNIL).

1. L'état du droit

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

Cette exigence a une importante toute particulière compte tenu du nombre d'entités qui seront assujetties aux stipulations de la directive, à savoir 15 000 selon l'étude d'impact du projet de loi. À ce titre, le paragraphe 4 de l'article 3 de la directive NIS 2 prévoit que les États membres peuvent mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes. L'auto-enregistrement est donc une simple faculté laissée aux États membres.

Les entités doivent communiquer 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 ;

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

2. Le dispositif proposé

Le **premier alinéa** attribue à l'ANSSI le rôle d'autorité auprès de laquelle les entités essentielles et importantes devront s'enregistrer. Celle-ci établira et mettra à jour la liste de ces entités et des bureaux d'enregistrement sur la base des informations qui lui seront communiquées par ces entités et bureaux d'enregistrement. De ce point de vue, il reviendra donc aux entités et aux bureaux d'enregistrement d'évaluer si elles entrent ou pas dans une des deux catégories.

Le **second alinéa** 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.

3. Les modifications apportées par le Sénat

Le Sénat a adopté quatre amendements à cet article, dont deux en commission et un en séance publique.

Un premier amendement, adopté en commission à l'initiative des rapporteurs, inscrit dans la loi la nécessité de mettre à jour *a minima* tous les deux ans la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement concernés par les dispositions du titre II du projet de loi, conformément au 5. de l'article 3 de la directive NIS 2.

Un second amendement, adopté en commission à l'initiative de Mme Audrey Linkenheld (Socialiste, Écologiste et Républicain), a introduit la nécessité que le décret en Conseil d'État pris pour l'application de cet article fasse l'objet d'un avis de la CNIL.

Un troisième amendement, adopté en séance publique à l'initiative de Mme Catherine Morin-Dessailly avec l'avis favorable de la commission et du gouvernement et sous-amendé par le gouvernement, prévoit que les informations transmises par les entités et les bureaux d'enregistrement à l'ANSSI doivent l'être « *dans le respect des modalités de chiffrement de bout en bout ainsi que de protection des données recueillies de l'effet des lois extraterritoriales* ». Cet ajout a été motivé par le fait que les informations communiquées à l'ANSSI revêtent souvent un caractère sensible et confidentiel et que, de ce fait, le partage des informations doit se faire dans des conditions de sécurité optimales. Le sous-amendement du gouvernement, adopté en séance publique, a supprimé les alinéas 1 à 3 de l'amendement de Mme Morin-Dessailly qui prévoyait que l'État, par l'intermédiaire de ses ministères, informe et sensibilise les entités concernées par la directive NIS 2 quant aux obligations qui leur incomberont.

4. La position de la commission

La commission spéciale a adopté quatre amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff visant à s'assurer de l'intégration des agents agissant pour le compte des bureaux d'enregistrement à la liste des entités établie par l'ANSSI tout en reprenant la terminologie utilisée dans le code des postes et des communications électroniques (CPCE) ;

– un amendement du président Philippe Latombe précisant que la liste des entités essentielles et importantes, des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers est communiquée après avis des ministères compétents pour les secteurs d'activité mentionnés à l'article 7 du projet de loi. L'objectif est que la liste en question soit la plus conforme possible à la réalité des secteurs d'activités concernés ;

– un amendement de M. Arnaud Saint-Martin et plusieurs de ses collègues du groupe LFI- NFP qui précise que le décret en Conseil d'État prévu à l'alinéa 2 fixant les informations à transmettre, leurs modalités de communication et les délais dans lesquelles les modifications doivent être transmises est pris après avis de la CNIL.

*

* *

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

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article prévoit les conditions dans lesquelles les dispositions du 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.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

- **Modifications apportées par la commission**

La commission a adopté deux amendements clarifiant les dispositions qui ne trouvent pas à s'appliquer dans le cas d'un acte sectoriel de l'Union européenne reconnu comme *lex specialis* qui prévoit des dispositions équivalentes. Il précise que sont uniquement concernées les dispositions relatives à l'application de mesures de sécurité, à la notification des incidents ainsi qu'à celles de la supervision permettant d'en vérifier le respect. En dehors de ces dispositions, les entités restent soumises au projet de loi.

1. L'état du droit

L'article 4 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, dite directive NIS 2, porte sur la compatibilité entre les dispositions de la directive et les autres actes juridiques sectoriels de l'Union européenne.

Il stipule 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 ne sont pas applicables auxdites entités.

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.

Cet article a notamment vocation à permettre la conciliation entre les stipulations de la directive NIS 2 et celles du règlement dit DORA et de la directive accompagnant ce règlement. Il devrait également s'appliquer à certaines entités relevant du secteur numérique, qui devront faire l'objet d'un règlement d'exécution spécifique de la Commission européenne.

Au plus tard le 17 juillet 2023, la Commission fournit des lignes directrices clarifiant l'application des paragraphes 1 et 2 de la directive[1].

2. Le dispositif proposé

L'article 13 du projet de loi transpose fidèlement les stipulations de l'article 4 de la directive.

Il convient de noter toutefois que la rédaction de l'article omet de transposer la stipulation de l'article 4 de la directive qui indique que lorsque des actes juridiques sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur

---

[1] *https://digital-strategy.ec.europa.eu/fr/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive*.

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.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui clarifie les dispositions qui ne trouvent pas à s'appliquer dans le cas d'un acte sectoriel de l'Union européenne reconnu comme *lex specialis* qui prévoit des dispositions équivalentes.

Il précise que sont uniquement concernées les dispositions relatives à l'application de mesures de sécurité, à la notification des incidents ainsi qu'à celles de la supervision permettant d'en vérifier le respect. En dehors de ces dispositions, les entités restent soumises au projet de loi, comme par exemple, l'obligation d'enregistrement issue de l'article 12 dont elles ne sont pas déliées.

*

* *

Article 14

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

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

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'information 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté quatre amendements à cet article.

Tout d'abord, le Sénat a adopté un amendement réécrivant l'alinéa 2 pour prévoir que les mesures que prennent les entités régulées visent notamment à faire en sorte 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.

Ensuite, il a complété l'alinéa 6 par un amendement précisant que le référentiel d'exigences techniques devra être adapté aux spécificités des différents acteurs mentionnés au premier alinéa de l'article, en fonction de leur degré d'exposition aux risques, de leur taille, de la probabilité de survenance d'incident et de leur gravité.

Un amendement a complété l'alinéa 6 pour imposer que le référentiel tienne compte des modalités de concertation des représentants des entités concernées et des associations d'élus.

Enfin, le Sénat a adopté un amendement de précision au début de l'alinéa 8 visant à circonscrire le périmètre des exigences de sécurité propres à certains opérateurs du numérique aux seuls d'entre eux qui sont des entités essentielles ou importantes.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté plusieurs amendements visant principalement à :

– exempter les entités dont les activités relèvent de la sécurité nucléaire ;

– prévoir que les entités mettent en œuvre à leurs frais les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services ;

– préciser que les mesures techniques et organisationnelles garantissent un niveau de résilience adapté et proportionné au risque ;

– renforcer les objectifs de sécurité et de résilience numérique en s'assurant que les mesures de cybersécurité prises par les entités critiques reposent sur des critères techniques objectifs ;

– indiquer que les membres des organes de direction ainsi que les personnes exposées aux risques doivent être formés à la cybersécurité en fonction de leur degré d'exposition au risque ;

– préciser que les mesures techniques, opérationnelles et organisationnelles doivent garantir la résilience des activités, des réseaux et des systèmes d'information ;

– ajouter les ministères à la liste des personnes avec lesquelles l'ANSSI se concerte pour l'élaboration, la modification et la publication du référentiel d'exigences techniques et organisationnelles ;

– offrir la possibilité pour les entités régulées de se prévaloir du recours à certaines prestations de services qualifiés, pour faciliter la démonstration de leur respect à tout ou partie des objectifs de sécurité.

1. L'état du droit

L'article 21 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, dite 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.

En outre, les mesures 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. Ces mesures sont fondées sur une approche dite « tous risques », qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents. Celles-ci comprennent :

– 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 d'hygiène numérique et la formation à la cybersécurité ;

– les 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 ;

– et 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.

2. Le dispositif proposé

L'article 14 du projet de loi transpose fidèlement les stipulations de l'article 21 de la directive, tout en apportant davantage de précisions quant aux obligations qui incombent aux différents acteurs assujettis.

Le **premier alinéa** précise que ces obligations s'appliquent :

– aux entités essentielles ;

– aux entités importantes ;

– 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 pour leurs réseaux de systèmes d'information ;

– au Commissariat à l'énergie atomique et aux énergies alternatives (CEA) pour ses activités dans le domaine de la défense ;

– et aux juridictions administratives et judiciaires.

Les **alinéas 1ers à 5**, qui ont trait aux mesures techniques, opérationnelles et organisationnelles que doivent prendre ces acteurs pour se conformer aux exigences, reprennent textuellement les mesures prévues à l'article 21 de la directive.

L'**alinéa 6** prévoit qu'un décret en Conseil d'État fixe les objectifs auxquels doivent se conformer les acteurs auxquels s'applique l'article 14 et détermine les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles adaptées à ces différents acteurs.

3. Les modifications apportées par le Sénat

Le Sénat a apporté quatre modifications à l'article 14.

Tout d'abord, le Sénat a adopté en commission un amendement des rapporteurs réécrivant l'**alinéa 2** pour prévoir que les mesures que prennent les entités régulées visent notamment à faire en sorte 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. L'objectif était d'insister sur la nécessité pour les organes de direction d'approuver et de superviser directement les mesures relatives à la cybersécurité.

Ensuite, il a complété l'**alinéa 6** par un amendement des rapporteurs adopté en commission en précisant que le référentiel d'exigences techniques devra être adapté aux spécificités des différents acteurs mentionnés au premier alinéa de l'article, en fonction de leur degré d'exposition aux risques, de leur taille, de la probabilité de survenance d'incident et de leur gravité. L'objectif était de renforcer le caractère strictement proportionné des obligations auxquelles devront se conformer les entreprises et les administrations publiques visées à l'article.

En séance publique, un amendement de Mme Linkenheld, qui a reçu un avis de sagesse de la commission et un avis favorable du gouvernement, a complété l'**alinéa 6** pour imposer que le référentiel tienne compte des modalités de concertation des représentants des entités concernées et des associations d'élus.

Enfin, le Sénat a adopté en séance publique un amendement de précision du gouvernement, qui avait reçu un avis favorable de la commission, au début de l'**alinéa 8** visant à circonscrire le périmètre des exigences de sécurité propres à certains opérateurs du numérique (fournisseurs de services de systèmes de noms de domaine, offices d'enregistrement, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données, fournisseurs de réseaux de diffusion du contenu, fournisseurs de services gérés, fournisseurs de services de sécurité gérés, fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux et prestataires de services de confiance) aux seuls d'entre eux qui sont des entités essentielles ou importantes.

4. La position de la commission

Outre quatre amendements rédactionnels de la rapporteure Anne Le Hénanff, la commission spéciale a adopté onze amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff exemptant les entités dont les activités relèvent de la sécurité nucléaire, pour lesquelles la France souhaite pouvoir exercer pleinement et entièrement sa compétence exclusive en matière de sauvegarde de la sécurité et de la souveraineté nationales ;

– un amendement de la rapporteure Anne Le Hénanff qui prévoit que les entités listées à l'alinéa premier de l'article 14 mettent en œuvre à leurs frais les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services ;

– un amendement du président Philippe Latombe qui précise que les mesures techniques et organisationnelles garantissent, pour leurs réseaux et leurs systèmes d'information, un niveau de résilience adapté et proportionné au risque ;

– un amendement du président Philippe Latombe qui vise à renforcer les objectifs de sécurité et de résilience numérique inscrits dans le projet de loi en s'assurant que les mesures de cybersécurité prises par les entités critiques reposent sur des critères techniques objectifs. Cet amendement s'inscrit dans la continuité de l'article 16 de la loi n° 2016-1321 pour une République numérique, qui dispose déjà que les administrations doivent veiller « *à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information* ». Il propose d'étendre cette exigence à l'ensemble des entités essentielles et importantes et de la traduire en cinq critères techniques objectifs : auditabilité, transparence, interopérabilité, pérennité et maitrise ;

– un amendement du président Philippe Latombe qui indique que les membres des organes de direction ainsi que les personnes exposées aux risques doivent être formés à la cybersécurité en fonction de leur degré d'exposition au risque ;

– un amendement de la rapporteure Anne Le Hénanff à l'alinéa 5 qui précise que les mesures techniques, opérationnelles et organisationnelles doivent garantir la résilience des activités, des réseaux et des systèmes d'information ;

– un amendement de la rapporteure Anne Le Hénanff à l'alinéa 6, qui, d'une part, ajoute les ministères à la liste des personnes avec lesquelles l'ANSSI se concertera pour l'élaboration, la modification et la publication du référentiel d'exigences techniques et organisationnelles, et d'autre part, procède à des modifications d'ordre rédactionnelles dans un but de clarification ;

– un amendement de la rapporteure Anne Le Hénanff à l'alinéa 8 qui clarifie cet alinéa en faisant référence explicitement au référentiel européen défini par le règlement d'exécution (UE) n° 2024/2690, pris en application de la directive NIS 2. Cette clarification garantit la cohérence entre le cadre européen et le dispositif national élaboré par l'ANSSI, prévu par décret en Conseil d'État, pour les entités concernées. Elle permet en outre d'écarter toute ambiguïté d'interprétation et de prévenir les risques de surtransposition ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff offrant la possibilité pour les entités régulées de se prévaloir du recours à certaines prestations de services qualifiés, pour faciliter la

démonstration de leur respect à tout ou partie des objectifs de sécurité. Il valorise le recours par les entités assujetties aux prestations qualifiées par l'ANSSI et favorise le développement de l'offre de confiance. Les entités régulées pourront en fonction de leurs besoins identifier les solutions qu'elles considèrent comme adéquates à leurs enjeux. Les conditions d'application des dispositions introduites par cet amendement seront prévues par décret en Conseil d'État.

*

* *

Article 15

Opposabilité à l'ANSSI en cas de contrôle de la mise en œuvre du référentiel d'exigences techniques et organisationnelles

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article rend 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Deux amendements ont été adoptés à cet article. Un premier amendement crée un mécanisme de reconnaissance mutuelle entre les États membres de l'Union européenne et vers d'autres types de référentiels, de sorte qu'une entité qui aurait vu certifiée sa conformité à un référentiel dont le niveau équivalent de sécurité a été validé par l'ANSSI, puisse s'en prévaloir à l'occasion d'un contrôle.

Un second amendement précise que la modalité de vérification par l'ANSSI de la conformité au référentiel d'exigences techniques peut se faire au moyen d'un label de confiance approuvé par elle.

➢ **Modifications apportées par la commission**

La commission spéciale a procédé à une réécriture quasi complète de l'article 15 afin de clarifier les conditions dans lesquelles seront reconnues les normes et spécifications techniques, européennes ou interationales permettant aux entités régulées de démontrer leur conformité à tout ou partie des objectifs visés. La nouvelle rédaction facilite par ailleurs, pour les entités établies dans plusieurs pays

au sein de l'Union européenne, la reconnaisance de leur conformité de tout ou partie des objectifs visés lorsqu'elles appliquent un autre référentiel que celui de l'ANSSI.

1. L'état du droit

L'article 15 du projet de loi ne transpose pas une stipulation 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, dite directive NIS 2. Il précise les modalités d'application de l'article 14 du projet de loi.

2. Le dispositif proposé

Le **premier alinéa** apporte des précisions quant au référentiel d'exigences techniques et organisationnelles prévu à l'article 14 du projet de loi, qui sera mis en place par décret en Conseil d'État. En particulier, il 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. L'objectif est de simplifier la procédure de contrôle du respect des exigences techniques par l'ANSSI. Cette simplification vaut d'ailleurs tant pour les acteurs contrôlés que pour l'ANSSI elle-même.

Le **second alinéa** dispose qu'à défaut de pouvoir opposer la mise en œuvre du référentiel que l'ANSSI prescrit, les personnes mentionnées à l'article 14 du projet de loi sont tenues de démontrer que les mesures qu'elles mettent en œuvre permettent de se conformer à ces objectifs.

3. Les modifications apportées par le Sénat

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 l'ANSSI mais qui serait reconnu par elle comme de même niveau que son propre référentiel, le Sénat a modifié le **premier alinéa** en commission, à l'initiative des rapporteurs, en créant un mécanisme de reconnaissance mutuelle entre les États membres de l'Union européenne. Ainsi, une entité qui aurait été jugée certifiée conforme aux exigences de la directive NIS 2 dans un autre État membre de l'Union européenne pourrait s'en prévaloir lors d'un contrôle de l'ANSSI.

Par ailleurs, le Sénat a précisé en séance publique, par un amendement du gouvernement qui a reçu l'avis favorable de la commission, que la modalité de vérification par l'ANSSI de la conformité au référentiel d'exigences techniques peut se faire au moyen d'un label de confiance approuvé par elle. Ce label n'existe pas encore et devrait donc être éventuellement créé, à l'initiative de l'ANSSI, si cette disposition législative demeurait.

4. La position de la commission

La commission spéciale a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui procèdent à une réécriture quasi complète de l'article 15 afin de clarifier les conditions dans lesquelles seront reconnues les normes et spécifications techniques, européennes ou interationales permettant aux entités régulées de démontrer leur conformité toute ou partie aux objectifs visés.

Cette nouvelle rédaction vise par ailleurs à faciliter, pour les entités établies dans plusieurs pays au sein de l'Union européenne, la reconnaisance de leur conformité de tout ou partie des objectifs visés lorsqu'elles appliquent un autre référentiel que celui de l'ANSSI.

*

* *

Article 16
Exigences de protection cyber supplémentaires pour les OIV et pour les administrations

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article confère 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.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat a adopté un seul amendement rédactionnel.

- **Modifications apportées par la commission**

La commission spéciale a adopté plusieurs amendements visant en particulier à corriger des erreurs rédactionnelles.

1. L'état du droit

Comme indiqué précédemment, l'article 21 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, dite 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.

2. Le dispositif proposé

En plus des dispositions de l'article 14 du projet de loi imposant des obligations en matière de cybersécurité, qui transposent les stipulations de l'article 21 de la directive NIS 2, l'article 16 prévoit des obligations supplémentaires pour rehausser le niveau de sécurité des opérateurs d'importance vitale (OIV) et de plusieurs catégories d'administrations.

En vertu de l'article L. 1332-1 du code de la défense, sont des OIV 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, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste [(1)] .

L'article L. 1332-2 du même code précise que les obligations prescrites aux OIV peuvent être étendues à des 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.

Le **premier alinéa** prévoit que les OIV doivent identifier, tenir à jour et communiquer à l'ANSSI la liste de leurs systèmes d'information d'importance vitale.

Le **deuxième alinéa** dispose que les OIV mettent en œuvre les mesures du référentiel d'exigences techniques prévu à l'article 14 du projet de loi et les exigences spécifiques à ces systèmes d'information fixées par le premier ministre.

---

(1) Cf. commentaire de l'article premier.

Le **troisième alinéa** liste les administrations qui devront mettre en œuvre les exigences du référentiel mentionné à l'article 14 ainsi que les exigences spécifiques du premier ministre.

Le **quatrième alinéa** prévoit que les exigences spécifiques peuvent inclure le recours à des dispositifs matériels et logiciels, à des prestataires de services certifiés, qualifiés ou agréés et prévoir que ce recours 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 à noter que les acteurs qui relèvent de l'article 16 appliquent ces exigences à leurs frais.

3. Les modifications apportées par le Sénat

Un amendement rédactionnel des rapporteurs Patrick Chaize, Hugues Saury et Michel Canévet a modifié l'alinéa 3 pour mettre en cohérence la rédaction de cet article avec la rédaction retenue aux articles 8 et 14 du projet de loi.

4. La position de la commission

La commission spéciale a adopté neuf amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui visent à corriger une erreur rédactionnelle. En tant qu'établissement public à caractère industriel et commercial, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), notamment pour ses activités dans le domaine de la défense, n'est en effet pas concerné par ces 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 ;

– et sept amendements rédactionnels de la rapporteure Anne Le Hénanff.

*

* *

Article 16 bis
Empêcher l'intégration de dispositifs techniques visant à affaiblir la sécurité des systèmes d'information et des communications électroniques

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article vise à empêcher l'intégration de dispositifs techniques dans les systèmes d'information et les systèmes de communications électroniques visant à affaiblir leur cybersécurité.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a introduit cet article additionnel en séance publique.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement qui insère les mots « *ou processus* » après le mot « *mécanisme* » afin d'élargir le champ de l'article 16 *bis*.

1. L'état du droit

● L'article L. 33-1 du code des postes et des communications électroniques (CPCE) pose le principe de liberté de l'établissement et de l'exploitation des réseaux ouverts au public et de la fourniture de services de communications électroniques.

Le I fixe néanmoins plusieurs limites : cette liberté s'exerce, en particulier, sous réserve « *des prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre* » (e du I de l'article L. 33-1 du CPCE).

● Le II de l'article L. 34-1 du CPCE impose aux opérateurs de communications électroniques, et notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, d'effacer ou de rendre anonymes les données relatives aux communications électroniques. De nouveau, plusieurs réserves sont prévues, énumérées aux II *bis* à VI de l'article.

Le II *bis* formule ainsi une obligation de conservation de certaines données et informations au regard de plusieurs finalités :

– pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, l'opérateur doit conserver les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de la validité du contrat qui le lie à celui-ci (1°). Il doit également, pour ces mêmes finalités, conserver les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte, selon le service de communication utilisé, ainsi que les

informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de la validité du contrat ou de la clôture du compte (2°) ;

– pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les opérateurs doivent conserver les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux (3°).

Le III étend l'obligation de conservation mentionnée au II. Ainsi, pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, le premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II *bis*, et de données de localisation précisées par décret en Conseil d'État. Cette injonction du Premier ministre peut être renouvelée si les conditions continuent d'être réunies.

Par ailleurs, le III *bis* prévoit que les données conservées par les opérateurs peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant d'un accès aux données relatives aux communications électroniques, à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données.

Le VI détermine le champ des données conservées et traitées en application de l'article L. 34-1. Celles-ci portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, les caractéristiques techniques des communications assurées par ces deniers et sur la localisation des équipements terminaux. En aucun cas, elles ne peuvent porter sur le contenu des correspondances échangées ou des informations consultées.

● Les obligations des opérateurs et fournisseurs de services sur internet sont également prévues par le titre VII du livre VIII du code de la sécurité intérieure (CSI).

L'article L. 871-1 du code de sécurité intérieure dispose que « *les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre dans un délai de soixante-douze heures aux agents autorisés dans les conditions prévues à l'article L. 821-4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies* ». Les « *agents autorisés dans les conditions prévues à l'article L. 821-4* » désignent, en pratique, les services de renseignement.

En outre, cet article dispose que « *les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en œuvre dans un délai de soixante-douze heures ces conventions* ».

Toutefois, il précise que la transmission des conventions permettant le déchiffrement des données transformées au moyen des prestations fournies par les personnes physiques ou morales qui fournissent les prestations de cryptologie visant à assurer une fonction de confidentialité est obligatoire « sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions ».

C'est précisément cette dernière disposition qui est au cœur des difficultés rencontrées par les services de renseignement. En effet, le recours par ces prestataires de techniques de chiffrement dit « de bout en bout » rend impossible l'accès au contenu des messageries chiffrées par les services de renseignement et par les prestataires en question. Il s'agit d'un niveau de confidentialité optimal, qui présente toutefois l'inconvénient de rendre impossible le déchiffrement des données chiffrées de bout en bout qui ont été interceptées par les services de renseignement.

Toutefois, les services de renseignement ont accès à ce qu'on appelle les « métadonnées », c'est-à-dire à l'ensemble des données « autour » de la donnée principale qu'est le message chiffré. Ainsi, grâce à ces métadonnées, les services de renseignement sont à même de savoir, par exemple, que deux individus ont échangé des messages, à une heure et à une date précise, à partir d'un lieu précis, et depuis des terminaux et un mode de connexion à internet précis. En revanche, ils ne seront pas en mesure de connaître le contenu du message, qui a été chiffré de bout en bout.

La convention de déchiffrement des données

Les conventions de déchiffrement sont un moyen de cryptologie, notion définie par l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique comme 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 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.

L'article 30 de cette même loi pose le principe général selon lequel « *l'utilisation des moyens de cryptologie est libre* ».

Aux termes de l'article L. 871-3, le ministre chargé des communications électroniques doit veiller à ce que les exploitants de réseaux ouverts au public de communications électroniques et les fournisseurs de services de communications électroniques au public prennent les mesures nécessaires pour assurer l'application, dans le respect de la défense nationale, de ces dispositions dans le cadre de la mise en œuvre des techniques de renseignement et des interceptions de correspondances et techniques spéciales d'enquête ordonnées par l'autorité judiciaire.

L'article L. 871-4 impose aux opérateurs et fournisseurs de services sur internet d'autoriser, à des fins de contrôle, les membres et les agents de la Commission nationale de contrôle des techniques de renseignement (CNCTR) mandatés à cet effet à entrer dans ceux de leurs locaux dans lesquels sont mises en œuvre des techniques de recueil de renseignement soumises à autorisation du premier ministre.

Les exigences essentielles mentionnées au 12° de l'article L. 32 du CPCE et le secret des correspondances ne sont opposables, selon l'article L. 871-5 du CSI, ni aux juridictions compétentes pour ordonner des interceptions ni au ministre chargé des communications électroniques.

L'article L. 871-6 du CSI détermine les modalités de coopération des opérateurs dans la mise en œuvre des techniques de recueil de renseignement suivantes :

– le recueil des données de connexion (article L. 851-1) ;

– le recueil en temps réel des informations, documents et adresses complètes de ressources sur internet utilisés par une personne, pour les seuls besoins de la prévention du terrorisme (article L. 851-2) ;

– la mise en place de traitements automatisés sur les données transitant par les réseaux des opérateurs, dits « technique de l'algorithme » (article L. 851-3) :

– le recueil des données techniques relatives à la localisation des équipements terminaux auprès d'un opérateur (article L. 851-4) ;

– le recueil direct des données techniques permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux (article L. 851-6) ;

– les interceptions de correspondances émises par la voie des communications électroniques (article L. 852-1) ;

– l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique (article L. 853-2).

Ainsi, ces opérations peuvent être réalisées dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de communications électroniques, dès lors que le premier ministre ou la personne spécialement déléguée par lui en a donné l'ordre, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs dans leurs installations respectives.

À cet égard, il convient de rappeler que la loi n° 2021-998 du 30 juillet 2021 relative à la prévention du terrorisme et au renseignement a étendu le champ des techniques de renseignement pour lesquelles l'autorité administrative peut requérir

le concours des opérateurs, en incluant les trois dernières techniques de la liste *supra*, mentionnées aux articles L. 851-6, L 852-1 et L. 853-2 du CSI.

Les opérateurs et fournisseurs de service sur internet concernés par cette obligation bénéficient d'une compensation financière de l'État, au regard des surcoûts identifiables et spécifiques auxquels ils sont éventuellement exposés pour répondre à la mise en œuvre des techniques de renseignement.

● Ces obligations des opérateurs et fournisseurs de services font l'objet d'une répression pénale spécifique.

Ainsi, selon l'article L. 881-1 du CSI, le fait pour une personne concourant à l'exécution d'une technique de recueil de renseignement de révéler l'existence de la mise en œuvre de cette technique est puni des peines réprimant les atteintes au secret professionnel prévues par :

– l'article 226-13 du code pénal, qui punit d'un an d'emprisonnement et de 15 000 euros d'amende la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire ;

– l'article 226-14 du même code, qui prévoit que l'article 226-13 n'est pas applicable dans les cas où la loi impose ou autorise la révélation du secret ni dans les cas prévus aux 1° à 5° de l'article ;

– l'article 226-31, qui détermine diverses peines complémentaires.

Par ailleurs, selon l'article L. 881-2 du CSI, le fait de ne pas déférer aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et 150 000 euros d'amende. Les mêmes peines répriment le fait pour un opérateur ou un fournisseur de services de refuser de communiquer les informations ou documents ou le fait de communiquer des renseignements erronés.

De plus, l'article 434-15-2 du code pénal punit de trois ans d'emprisonnement et 270 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités. Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 euros d'amende.

2. Les modifications apportées par le Sénat

Le Sénat a introduit cet article additionnel en séance publique à l'initiative de M. Olivier Cadic. Cet amendement a été adopté au Sénat, contre l'avis de la commission et du gouvernement, dans le contexte de l'examen d'un article

additionnel après l'article 8 de la proposition de loi dite « Narcotrafic » qui avait été adopté en commission au Sénat. Après avoir été adopté en commission au Sénat, cet article additionnel, 8 *ter*, a été supprimé en commission des Lois à l'Assemblée nationale et n'a pas été rétabli à l'occasion de son examen en séance publique. Il n'a pas non plus été rétabli en commission mixte paritaire.

Dans un contexte de généralisation du recours aux protocoles de chiffrement de bout en bout pour garantir la confidentialité des données, l'article 16 *bis* dispose qu'« *il ne peut être imposé aux fournisseurs de services de chiffrement […] l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques* » afin d'empêcher « *[tout] accès non consenti aux données protégées* ». Cette disposition s'applique également aux prestataires de services de confiance qualifiés.

L'objectif de cet article est d'interdire l'introduction de « portes dérobées », c'est-à-dire de vulnérabilités informatiques volontairement introduites par les concepteurs des systèmes d'information et des services de communications électroniques pour permettre aux services de renseignement d'accéder au contenu des messageries chiffrées.

L'exposé sommaire de l'amendement ayant introduit cet article additionnel indique que « *certaines initiatives législatives et réglementaires, tant au niveau national qu'international, ont cherché à imposer aux fournisseurs de services de chiffrement des obligations visant à insérer des dispositifs techniques permettant un accès aux données protégées par des tiers, notamment par les autorités publiques* ».

Il ajoute en outre que « *ces dispositifs créent des vulnérabilités exploitables non seulement par les autorités prévues, mais également par des acteurs malveillants, qu'il s'agisse de cybercriminels, d'États hostiles ou d'entités privées cherchant à compromettre la sécurité des systèmes d'information* ».

3. La position de la commission

La commission a adopté un amendement du président Philippe Latombe, avec l'avis favorable de la rapporteure Anne Le Hénanff et défavorable du rapporteur général, qui insère les mots « *ou processus* » après le mot « *mécanisme* ». Cette insertion a pour objectif d'élargir le champ de l'article 16 *bis* pour inclure, au-delà des outils techniques tels que les portes dérobées ou les clés maitresses, des pratiques telles que la création d'un accès non consenti aux données protégées ou la mise en place d'un protocole de remise systématique de copies de clés privées qui, *in fine*, auraient le même effet que les outils techniques précités.

*

* *

Article 17
Obligation de notification à l'ANSSI des incidents importants

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit que les entités régulées au titre de la directive dite 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a apporté plusieurs modifications substantielles à l'article 17.

Tout d'abord, il a introduit les critères pour considérer qu'un incident est important au sens de la directive.

Par ailleurs, ont été introduits des délais de notification au *Computer Emergency Response Team* (CERT) national des incidents informatiques qui figurent à l'article 23 de la directive mais qui ne figuraient pas dans l'article 17 du projet de loi.

De plus, a été introduite à l'alinéa 11 l'obligation figurant au paragraphe 5 de l'article 23 prévoyant que le CERT fournit, sans retard injustifié et si possible dans les heures suivant la réception de l'alerte précoce en cas de cyberattaque, 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.

Enfin, a été supprimée la notion d'incident « critique », pour se limiter à la seule notion d'incident « important » prévu dans la directive.

En séance publique, un amendement a complété l'alinéa 14 de l'article en précisant la nature des incidents importants devant être notifiés sans retard injustifié.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant principalement à :

– préciser qu'un incident est considéré comme important uniquement s'il a causé ou est susceptible de causer des pertes financières « *significatives* » ;

– reprendre la rédaction de la directive NIS 2 qui régit les obligations des États membres et des entités en matière d'information aux destinataires des services lorsque l'entité essentielle ou importante identifie qu'une vulnérabilité critique est susceptible de les affecter et à clarifier le champ des informations devant leur être communiquées ;

– préciser à qui sont notifiés les incidents importants et les vulnérabilités critiques.

1. L'état du droit

La réponse à des incidents informatiques en France s'articule autour de l'ANSSI, et tout particulièrement de son centre de réponse aux incidents de sécurité CERT qui assure les fonctions de CERT à l'échelle nationale. À ce titre, les incidents informatiques affectant les opérateurs d'importance vitale (OIV), les opérateurs de services essentiels (OSE) et les opérateurs de communications électroniques doivent systématiquement être notifiés à l'ANSSI en vertu de la loi n° 2018-133 de transposition de la directive dite NIS 1. En plus du CERT de l'ANSSI, des centres de réponse aux incidents de sécurité informatique (CSIRT) régionaux, sectoriels et ministériels ont été créés. Ils contribuent également à la notification d'incidents, à l'aide à la remédiation ainsi qu'à la connaissance de l'état de la menace et à la sensibilisation face au risque cyber.

L'article 11 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, dite directive NIS 2, confie au CERT **national** la tâche de surveiller et d'analyser les cybermenaces au niveau national et, sur demande, d'apporter une assistance aux entités essentielles et importantes concernées pour surveiller leurs réseaux et systèmes d'information (paragraphe 3).

Le paragraphe 2 de l'article 23 de la directive prévoit 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 mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace.

Le paragraphe 3 de l'article 23 de la directive définit également 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.

La notion d'incident important a également été précisée dans le règlement d'exécution (UE) 2024/2690 du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, 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 et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

2. Le dispositif proposé

Le **premier alinéa** dispose que les personnes mentionnées à l'article 14 du projet de loi notifient sans retard injustifié à l'ANSSI tout incident ayant un impact important sur la fourniture de leurs services.

En cas de cyberattaque ayant affecté une entité essentielle ou une entité importante, l'ANSSI peut exiger de celles-ci qu'elles informent le public de l'incident dont elles ont été la cible ou le faire elle-même, dans le but de prévenir un incident ou pour faire face à un incident en cours ou lorsque la divulgation de l'incident est dans l'intérêt du public (**alinéa 12**).

L'alinéa 15 prévoit par ailleurs que les entités essentielles et importantes notifient sans retard 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.

L'alinéa 16 prévoit que l'obligation de notification ne s'étend pas aux informations dont la divulgation porterait atteinte aux intérêts de la défense et de la sécurité nationale.

L'alinéa 17 prévoit qu'en cas d'incident important ou de vulnérabilité critique, les personnes mentionnées au premier alinéa peuvent communiquer à l'ANSSI la liste des destinataires de leurs services. Celle-ci doit tenir 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'alinéa 18** prévoit que l'ANSSI informe la Commission nationale de l'informatique et des libertés (CNIL) de tout incident mentionné au premier alinéa susceptible d'entraîner une violation de données à caractère personnel.

Enfin, un décret en Conseil d'État fixe les modalités d'application du présent article. Il précise notamment la procédure applicable et les critères d'appréciation des caractères importants et critiques des incidents et vulnérabilités (**alinéa 19**).

3. Les modifications apportées par le Sénat

Le Sénat a apporté plusieurs modifications substantielles à l'article 17.

Tout d'abord, dans l'article, aux **alinéas 2 à 4**, il a introduit les critères pour considérer qu'un incident est important au sens de la directive. Cet amendement, à l'initiative des rapporteurs Patrick Chaize, Hugues Saury et Michel Canévet, a été adopté en commission.

Par ailleurs, toujours *via* cet amendement, ont été introduits aux **alinéas 5 à 10** des délais de notification au CERT national des incidents informatiques qui figurent à l'article 23 de la directive mais qui ne figuraient pas dans l'article 17 du projet de loi. Ces délais de notification devaient initialement être précisés par décret mais le Sénat a estimé que leur introduction dans la loi était indispensable.

Le séquençage prévu par le Sénat est le suivant :

– dans les 24 premières heures, une notification initiale qui, le cas échéant, indique si l'incident important est susceptible d'avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact en dehors du territoire national (**alinéa 6**) ;

– dans les 72 heures, une notification intermédiaire qui, le cas échéant, met à jour les informations communiquées à l'occasion de la notification initiale, et qui fournit une évaluation initiale de l'incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission lorsqu'ils sont disponibles (**alinéa 7**) ;

– dans le mois, un rapport final, sous réserve que l'incident soit traité (**alinéa 9**) ;

Par ailleurs, à la demande de l'ANSSI, l'entité peut être amenée à établir un rapport sur les mises à jour pertinentes (**alinéa 8**).

De plus, a été introduite à l'**alinéa 11** l'obligation figurant au paragraphe 5 de l'article 23 prévoyant que le CERT fournit, sans retard injustifié et si possible dans les heures suivant la réception de l'alerte précoce en cas de cyberattaque, 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.

Enfin, a été supprimée la notion d'incident « critique », pour se limiter à la seule notion d'incident « important » prévu dans la directive.

En séance publique, un amendement du gouvernement ayant reçu un avis favorable de la commission a précisé la nature des incidents importants devant être notifiés sans retard injustifié en complétant l'alinéa 14 par les mots « *ayant un impact direct sur les destinataires de leurs services, notamment lorsqu'ils ont causé ou sont susceptibles de causer l'extraction de données sensibles de ces derniers, ou de causer la mort ou des dommages considérables à la santé d'une personne physique destinataire, ou qu'ils consistent en un accès non autorisé effectif au réseau et aux systèmes d'information de l'entité, susceptible d'être malveillant et de causer une perturbation opérationnelle grave pour le destinataire* ». Cet amendement de sécurisation juridique vise à clarifier les types d'incidents importants que les entités devront notifier aux destinataires de leurs services afin de se conformer aux stipulations de l'article 23 de la directive qui soumet cette notification à la détermination de son caractère approprié.

4. La position de la commission

Outre six amendements rédactionnels de la rapporteure Anne Le Hénanff, la commission spéciale a adopté trois amendements :

– un amendement du président Philippe Latombe qui précise qu'un incident est considéré comme important uniquement s'il a causé ou est susceptible de causer des pertes financières « *significatives* » ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui reprennent la rédaction du 2. de l'article 23 de la directive NIS 2 qui régit les obligations des États membres et des entités en matière d'information aux destinataires des services lorsque l'entité essentielle ou importante identifie qu'une vulnérabilité critique est susceptible de les affecter. Ils clarifient également le champ des informations devant leur être communiquées en s'alignant sur le même article de la directive NIS 2 qui limite le champ des informations communiquées aux destinataires aux mesures et corrections que les utilisateurs peuvent appliquer, et, le cas échéant, les informations relatives à la vulnérabilité elle-même. Enfin, ils précisent la rédaction du projet de loi qui n'indique pas à qui sont notifiés les incidents importants et les vulnérabilités critiques.

*

* *

Section 3
Enregistrement des noms de domaine

Article 18
Détermination des critères territoriaux pour l'application aux offices et aux bureaux d'enregistrement des noms de domaine

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article définit par des critères de compétence territoriaux les offices et les bureaux d'enregistrement auxquels s'appliquent les dispositions de la section 3 « Enregistrement des noms de domaine » du projet de loi.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

- **Modifications apportées par la commission**

La commission a adopté un amendement rédactionnel.

1. L'état du droit

Le cadre juridique relatif aux noms de domaine est aujourd'hui fixé par les articles L. 45 à L. 48 du code des postes et des communications électroniques.

De ce point de vue, 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 directive NIS 2, opère un changement important en intégrant en 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.

En effet, l'article 28 stipule qu'afin de contribuer à la sécurité, à la stabilité et à la résilience du *Domain Name System* (DNS), 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 collecter les données d'enregistrement de noms de 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.

Les autorités chargées de la sécurité des systèmes d'information ou les autorités judiciaires pourront ainsi 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.

Pour ce faire, les États membres devront donc imposer aux offices d'enregistrement de collecter ou de conserver certaines données d'enregistrement des noms de domaine et organiser l'accès à ces données aux autorités légitimes.

2. Le dispositif proposé

L'article 18 du projet de loi dispose que les offices d'enregistrement et les bureaux d'enregistrement ainsi que les agents agissant pour le compte de ces derniers qui satisfont à l'une des conditions prévues à l'article 11 du projet de loi [(1)] sont soumis aux dispositions de la section 3 relative à l'enregistrement des noms de domaine, dont l'objet est de transposer les stipulations de l'article 28 de la directive.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission a adopté un amendement rédactionnel de la rapporteure Anne Le Hénanff.

*

* *

(1) Cf. commentaire de l'article 11.

Article 19

Obligation pour les offices et les bureaux d'enregistrement des noms de domaine de mettre en place une base de données

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article oblige les offices et les bureaux d'enregistrement des noms de domaine à 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant à :

– compléter l'alinéa 1er par les mots : « *y compris les données du point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire, notamment en cas de recours à des services permettant l'anonymisation des données d'enregistrement* » ;

– appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations en matière de protection des données prévues à l'alinéa 2 ;

– indiquer que les procédures de vérification des données n'ont pas pour objectif de s'assurer de l'exactitude de ces données au moment de leur collecte ;

– spécifier le contenu du décret mentionné à l'alinéa 3.

1. L'état du droit

L'article 28 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, dite directive NIS 2, prévoit de nouvelles règles en matière d'enregistrement des noms de domaine (1) .

(1) Cf. commentaire de l'article 18.

En vertu de cet article, afin de contribuer à la sécurité, à la stabilité et à la résilience du *Domain Name System* (DNS), 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 collecter les données d'enregistrement de noms de 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 de la directive 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 ses coordonnées sont différentes de celles du titulaire du nom de domaine.

En outre, les États membres doivent exiger 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 visées au paragraphe 1 contiennent des informations exactes et complètes. Les États membres imposent que ces politiques et procédures soient mises à la disposition du public.

De plus, 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.

Enfin, le paragraphe 6 de l'article 28 de la directive précise que les États membres imposent aux registres de noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine de coopérer entre eux.

2. Le dispositif proposé

L'article 19 transpose les obligations prévues à l'article 28 de la directive. En particulier, l'**alinéa premier**, qui 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, transpose les stipulations du paragraphe 1 de l'article 28 de la directive.

Les offices et les bureaux d'enregistrement ont l'obligation de maintenir ces bases de données à jour, en maintenant les données exactes et complètes, sans redondance de collecte, prévue au paragraphe 1 de l'article 28 de la directive et à l'**alinéa 2**. 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.

Enfin, un décret en Conseil d'État, pris après avis de la CNIL, fixe la liste des données relatives aux noms de domaine devant être collectées (**alinéa 3**).

3. Les modifications apportées par le Sénat

Le Sénat n'a apporté que des modifications d'ordre légistique.

4. La position de la commission

Outre un amendement rédactionnel de la rapporteure Anne Le Hénanff, la commission spéciale a adopté dix amendements :

– quatre amendements identiques portés par le rapporteur général Éric Bothorel, M. Denis Masséglia, M. René Pilato et plusieurs de ses collègues membres du groupe LFI-NFP, ainsi que Mme Marie Récalde et plusieurs de ses collègues du groupe Socialistes et apparentés, qui garantissent le fait que l'ensemble des informations relatives au titulaire du nom de domaine, y compris lorsque ce dernier fait appel à un service tiers, sont bien récupérées par les bureaux et offices d'enregistrement au stade de la collecte, en cohérence avec l'article 28 de la directive qui prévoit la collecte des informations « *du point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire* » ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui visent, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations en matière de protection des données prévues à l'alinéa 2 ;

– deux amendements de la rapporteure Anne Le Hénanff et de M. Antoine Villedieu qui clarifient le fait que les procédures de vérification des données n'ont pas pour objectif de s'assurer de l'exactitude de ces données au moment de leur collecte. En effet, les offices et bureaux d'enregistrement n'ont pas les capacités

d'effectuer une telle vérification au moment même de la collecte pour l'ensemble des noms de domaine ;

– deux amendements de M. Denis Masséglia et de M. René Pilato et plusieurs de ses collègues membres du groupe LFI-NFP qui visent à spécifier le contenu du décret mentionné à l'alinéa 3 en indiquant que celui-ci devra préciser les procédures de vérification des données d'enregistrement des noms de domaine menées par les bureaux et les offices d'enregistrement.

*

* *

Article 20

Durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaine

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

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 de domaine est utilisé.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Un amendement a modifié le délai de conservation des données en étendant celle-ci à la durée d'utilisation du nom de domaine et jusqu'à l'expiration d'un délai d'un an à compter de la cessation de l'utilisation de ce nom de domaine.

➢ **Modifications apportées par la commission**

La commission a adopté deux amendements qui visent, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations prévues au présent article portant sur la durée de conservation des données relatives à chaque nom de domaine.

1. L'état du droit

L'article 28 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, dite directive NIS 2, ne prévoit pas de durée de conservation des données collectées par les offices et les bureaux d'enregistrement des noms de domaine.

Toutefois, pour que les stipulations de l'article 28 de la directive puissent s'appliquer, en particulier celles relatives à l'obligation de collecter ces données et de les maintenir exactes et complètes au sein d'une base de données prévue à cet effet, la fixation d'une durée de conservation semble opportune.

2. Le dispositif proposé

Cet article prévoyait initialement que les offices et les bureaux d'enregistrement des noms de domaine conservent les données relatives à chaque nom de domaine dans leur base de données tant que le nom de domaine est utilisé.

3. Les modifications apportées par le Sénat

Un amendement de Mme Sylvie Robert (Socialiste, Écologiste et Républicain) adopté en séance publique a modifié le délai de conservation des données en étendant celle-ci à la durée d'utilisation du nom de domaine et jusqu'à l'expiration d'un délai d'un an à compter de la cessation de l'utilisation de ce nom de domaine, pour éviter l'acquisition multiple de noms de domaine par un même acteur dans des intervalles de temps réduits.

4. La position de la commission

La commission spéciale a adopté deux amendements du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui visent, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations prévues au présent article portant sur la durée de conservation des données relatives à chaque nom de domaine.

*

* *

Article 21

Obligation de publication des données d'enregistrement d'un nom de domaine

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article oblige les offices et les 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté deux amendements qui visent, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement l'obligation de publication des données d'enregistrement qui n'ont pas de caractère personnel prévue au présent article .

1. L'état du droit

Le paragraphe 4 de l'article 28 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, dite 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.

2. Le dispositif proposé

Cet article transpose les stipulations du paragraphe 4 de l'article 28 de la directive en prévoyant que les offices et bureaux d'enregistrement 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. Il reprend donc quasiment mot à mot le paragraphe 4 de l'article 28 de la directive.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui visent, en conformité avec la directive, à appliquer aux agents agissant pour le compte des bureaux d'enregistrement l'obligation de publication des données d'enregistrement qui n'ont pas de caractère personnel prévue à l'article 21 du projet de loi.

*

* *

Article 22

Obligation de communiquer les données collectées par les offices et les bureaux d'enregistrement à l'autorité judiciaire et à l'ANSSI pour les besoins des procédures pénales ou de la sécurité des systèmes d'information

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit que les offices et les bureaux d'enregistrement devront mettre en place des procédures permettant aux services de l'État d'accéder aux données collectées relatives aux noms de domaine, à leur demande, dans un délai maximal de 72 heures.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant à :

– appliquer aux agents agissant pour le compte des bureaux d'enregistrement les obligations prévues au présent article , portant sur la communication des données

relatives aux noms de domaine aux agents habilités à cet effet par l'autorité judiciaire ;

– préciser que, dans le cadre d'infractions au droit de la propriété intellectuelle, deux catégories d'agents doivent être spécialement habilités pour solliciter un accès aux données d'enregistrement des noms de domaines, en plus de ceux figurant déjà à l'article 22 : les agents assermentés et les commissaires de justice.

1. L'état du droit

Le paragraphe 5 de l'article 28 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, dite 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, il 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, les États membres imposent que les politiques et procédures de divulgation de ces données soient rendues publiques.

2. Le dispositif proposé

Le **premier alinéa** prévoit que les agents habilités à cet effet par l'autorité judiciaire ou par l'ANSSI peuvent obtenir des offices et bureaux d'enregistrement les données mentionnées à l'article 20 pour les besoins des procédures pénales et de la sécurité des systèmes d'information.

En outre, l'**alinéa 2** prévoit que les offices et les bureaux d'enregistrement fixent les règles de procédure pour la communication de ces données, qui doit intervenir dans un délai n'excédant pas 72 heures. Ces règles sont accessibles au public.

Enfin, un décret en Conseil d'État, pris après avis de la CNIL, fixera les modalités d'application de l'article (**alinéa 3**).

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

Outre trois amendements rédactionnels de la rapporteure Anne Le Hénanff, la commission spéciale a adopté trois amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui appliquent aux agents agissant pour le compte des bureaux d'enregistrement les obligations prévues à l'article 22 du projet de loi, portant sur la communication des données relatives aux noms de domaine aux agents habilités à cet effet par l'autorité judiciaire ;

– un amendement de M. Denis Masséglia qui précise que, dans le cadre d'infractions au droit de la propriété intellectuelle, deux catégories d'agents doivent être spécialement habilités pour solliciter un accès aux données d'enregistrement des noms de domaines, en plus de ceux figurant déjà à l'article 22 : les agents assermentés mentionnés à l'article L. 331.2 du code de la propriété intellectuelle, c'est-à-dire des agents d'organismes autorisés par la loi à dresser des procès-verbaux constatant des faits susceptibles d'une qualification pénale au titre de leur mission de lutte contre la contrefaçon, et les commissaires de justice de l'article 1er de l'ordonnance 2016-728 du 2 juin 2016 modifiée par la loi n° 2023-1059 du 20 novembre 2023, c'est-à-dire des auxiliaires de justice qualifiés par la loi à dresser ces mêmes procès-verbaux, dans le cas présent, en matière d'atteinte aux droits de la propriété intellectuelle. La finalité de cet amendement est de combattre les utilisations abusives du système d'enregistrement de noms de domaine pour mener des activités illégales et préjudiciables.

*

* *

Section 4
Coopération et échanges d'informations

Article 23
Dérogation aux secrets protégés par la loi pour la communication d'informations en matière de cybersécurité entre l'ANSSI et ses interlocuteurs

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article déroge 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté deux amendements identiques prévoyant que la communication d'informations ne peut intervenir que si elle est nécessaire à l'accomplissement des missions des personnes émettrices ou destinataires de ces informations. En outre, les informations échangées doivent se limiter au strict nécessaire et doivent être proportionnées à l'objectif du partage ; ce qui était, du reste, prévu par la directive. Enfin, le partage des informations doit préserver la confidentialité des informations en question et protéger la sécurité et les intérêts commerciaux des entités concernées.

➢ **Modifications apportées par la commission**

Outre un amendement rédactionnel, la commission spéciale a adopté un amendement destiné à éviter l'introduction de la notion d'intérêts commerciaux dans la loi.

1. L'état du droit

Le paragraphe 13 de l'article 2 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, dite

directive NIS 2, prévoit que sans préjudice de l'article 346 du Traité sur le fonctionnement de l'Union européenne, les informations considérées comme confidentielles en application de la réglementation de l'Union ou nationale, 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 présente directive.

Les 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. Ainsi, ces informations confidentielles peuvent faire l'objet d'échanges pour permettre l'application de la directive mais à la condition de les limiter au strict nécessaire et que ce partage soit proportionné à l'objectif de l'échange.

En outre, le paragraphe 11 de l'article 2 de la directive 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.

2. Le dispositif proposé

Cet article transpose les stipulations des paragraphes 11 et 13 de l'article 2 de la directive. Celui-ci vise :

– à définir un cadre en matière de coopération et d'échange d'informations en matière de cybersécurité ;

– à déroger, dans cette perspective, aux secrets protégés par la loi et au secret de l'instruction ;

– et, dans le même temps, à apporter des garanties suffisantes à la sécurité nationale, la sécurité publique ou la défense nationale.

Ainsi, le **premier alinéa** prévoit que les dispositions de l'article 11 du code de procédure pénale ou celles relatives aux autres 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, 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, entre, d'une part, l'ANSSI, et, d'autre part, la CNIL ou les autorités compétentes chargées de la gestion des risques en matière de cybersécurité en vertu d'un acte sectoriel de l'Union européenne ou les autorités chargées de la conduite de la politique pénale, de l'action publique et de l'instruction ou la Commission européenne ou les autorités compétentes des autres États membres de l'Union européenne ou des

CSIRT ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information.

Par conséquent, l'échange d'informations exclut directement la communication d'informations couvertes par le secret de la défense nationale. En revanche, les informations relevant du secret des affaires peuvent être communiquées, tout comme les données à caractère personnel au sens du règlement général sur la protection des données.

Les modalités d'application de l'article, notamment celles relatives au partage d'informations, sont déterminées par un décret en Conseil d'État (**alinéa 3**).

3. Les modifications apportées par le Sénat

Le Sénat a adopté deux amendements identiques en commission à l'initiative de Mme Morin-Desailly et de Mme Paoli-Gagin. Ces amendements prévoient que la communication d'informations ne peut intervenir que si elle est nécessaire à l'accomplissement des missions des personnes émettrices ou destinataires de ces informations. En outre, les informations échangées doivent se limiter au strict nécessaire et doivent être proportionnées à l'objectif du partage ; ce qui était, du reste, prévu par la directive. Enfin, le partage des informations doit préserver la confidentialité des informations en question et protéger la sécurité et les intérêts commerciaux des entités concernées.

4. La position de la commission

La commission spéciale a adopté deux amendements de la rapporteure Anne Le Hénanff : un amendement rédactionnel et un amendement destiné à éviter l'introduction de la notion d'intérêts commerciaux dans la loi, notion dont les contours ne sont pas déterminés en droit français, lequel connaît en revanche celle de secret des affaires. L'objectif de cet amendement est que le partage d'information puisse avoir lieu entre les autorités compétentes dans la mesure nécessaire à l'exercice des missions qui leur sont confiées par les textes, les garanties de confidentialité et de partage limité à ce qui est justifié figurent dans le texte et sont de nature à répondre aux prescriptions de la directive NIS 2.

*

* *

Article 24

Agrément par l'ANSSI d'organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents cyber

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

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.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

- **Modifications apportées par la commission**

La commission a adopté un amendement rédactionnel.

1. L'état du droit

L'article 24 du projet de loi ne transpose pas directement un article 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, dite directive NIS 2, mais participe de l'effort de structuration du réseau des CSIRT et CERT placés sous l'autorité de l'ANSSI.

2. Le dispositif proposé

L'article 24 du projet de loi prévoit que l'ANSSI agrée des organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents de cybersécurité. S'agissant des relais privés, c'est déjà le cas depuis longtemps : l'ANSSI agrée des prestataires de réponse à incidents (PRIS) qui interviennent pour rétablir les systèmes d'informations d'acteurs publics ou privés victimes de cyberattaques.

Par ailleurs, il prévoit que l'ANSSI et les organismes qu'elle agrée peuvent échanger entre eux des informations couvertes par des secrets protégés par la loi.

Les modalités d'application de cet article seront précisées par un décret en Conseil d'État.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté un amendement rédactionnel de la rapporteure Anne Le Hénanff.

*

* *

CHAPITRE III
De la supervision

Article 25
Prescription par l'ANSSI de mesures nécessaires en cas de cybermenaces

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article autorise 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.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement rédactionnel.

- **Modifications apportées par la commission**

La commission a adopté des amendements étendant aux agents agissant pour le compte des bureaux d'enregistrement les dispositions de l'article 25, en cohérence avec l'intégration des bureaux d'enregistrement au sein de cet article.

1. L'état du droit

L'article 21 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, dite 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.

2. Le dispositif proposé

Si la transposition de l'article 21 de la directive NIS 2 est assurée par l'article 14 du projet de loi, le présent article confère également à l'ANSSI des pouvoirs lorsqu'elle a connaissance d'une menace susceptible de porter atteinte aux entités régulées au titre de la directive.

En effet, lorsque l'ANSSI aura connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des entités mentionnées à l'article 14 et des bureaux d'enregistrement, elle pourra prescrire à la personne ou au bureau d'enregistrement concerné les mesures nécessaires pour éviter un incident ou y remédier et déterminer les délais accordés pour les mettre en œuvre et en rendre compte (**premier alinéa**).

En outre, un décret en Conseil d'État précisera les modalités d'application de l'article (**alinéa 2**).

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement rédactionnel à l'initiative des rapporteurs complétant l'alinéa 1er de l'article en insérant les mots « pour éviter un incident ou y remédier et déterminer les délais accordés pour les mettre en œuvre et en rendre compte » après les mots « mesures nécessaires ».

4. La position de la commission

La commission a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui visent à étendre aux agents agissant pour le compte des bureaux d'enregistrement les dispositions de l'article 25, en cohérence avec l'intégration des bureaux d'enregistrement au sein de cet article. Cette intégration se justifie par les besoins opérationnels de l'ANSSI pour éviter ou remédier à un incident.

*

* *

Section 1
Recherche et constatation des manquements

Article 26 A
(art. L. 103 du code des postes et des communications électroniques)
Services de coffre-fort numérique

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article complète l'avant-dernier alinéa de l'article L. 103 du code des postes et des communications électroniques (CPCE) en substituant à la mention « *établie selon un* » la mention « *lorsqu'il répond aux prescriptions d'un* ». Cet article ne transpose pas un article de la directive dite NIS 2.

➢ **Dernières modifications législatives intervenues**

L'article L. 103 du CPCE est entré en vigueur le 6 octobre 2017. Il a été modifié par l'article 14 de l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel qui a remplacé à l'alinéa 4 de l'article les mots « *accord exprès* » par le mot « *consentement* ».

➢ **Modifications apportées par le Sénat**

Cet article a été introduit en commission par un amendement des rapporteurs MM. Patrick Chaize, Hugues Saury et Michel Canévet.

➢ **Modifications apportées par la commission**

La commission spéciale a supprimé la certification par l'ANSSI des services de coffre-fort numérique.

1. L'état du droit

L'article L. 103 du CPCE a trait aux services de coffre-fort numérique. Il correspond à un service en ligne permettant de stocker de manière dématérialisée et de protéger tous les documents importants d'une entreprise et de ses salariés. Seules les personnes disposant des codes d'accès peuvent ajouter, supprimer, consulter ou modifier un document stocké dans ce coffre-fort numérique.

En vertu de l'article L. 103, un service de coffre-fort numérique est un service qui a pour objet :

– la réception, le stockage, la suppression et la transmission de données ou documents électroniques dans des conditions permettant de justifier de leur intégrité et de l'exactitude de leur origine ;

– la traçabilité des opérations réalisées sur ces documents ou données et la disponibilité de cette traçabilité pour l'utilisateur ;

– l'identification de l'utilisateur lors de l'accès au service par un moyen d'identification électronique ;

– de garantir l'accès exclusif aux documents électroniques, données de l'utilisateur ou données associées au fonctionnement du service à cet utilisateur, aux tiers autres que le prestataire de service de coffre-fort numérique, explicitement autorisés par l'utilisateur à accéder à ces documents et données et, le cas échéant, au prestataire de service de coffre-fort numérique réalisant un traitement de ces documents ou données au seul bénéfice de l'utilisateur et après avoir recueilli son consentement dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

– et de donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine, dans des conditions définies par décret.

Ce service de coffre-fort numérique peut bénéficier d'une certification établie selon un cahier des charges proposé par l'ANSSI après avis de la CNIL et approuvé par arrêté du ministre chargé du numérique.

2. Le dispositif proposé

L'article 26 A complète l'avant-dernier alinéa de l'article L. 103 du CPCE en substituant à la mention « *établie selon un* » la mention « *lorsqu'il répond aux prescriptions d'un* ». Cet article ne transpose pas un article de la directive dite NIS 2.

3. Les modifications apportées par le Sénat

Le Sénat a introduit cet article par voie d'amendement des rapporteurs. Il s'agit d'un amendement de coordination.

4. La position de la commission

La commission a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui suppriment la certification par l'ANSSI des services de coffre-fort numérique, pour trois raisons :

– les dispositions prévues aux 1° à 5° de l'article L. 103 du CPCE permettent de garantir un niveau de sécurité minimal, jugé suffisant par l'ANSSI, pour les services de coffre-fort numérique s'accompagnant d'un régime de sanction porté par l'article L. 122-22 du code de la consommation ;

– la certification de ces services de coffre-fort numérique, introduite à l'avant-dernier alinéa de l'article L. 103 du CPCE, n'est pas obligatoire pour les fournisseurs de tels services. Par ailleurs, aucun cas d'usage nécessitant le recours à un service de coffre-fort numérique certifié n'est identifié. Par conséquent, aucun autre cadre légal ou règlementaire ne prévoit d'imposer le recours à de tels services certifiés ;

– la mise en place d'une telle certification représente un coût aussi bien pour l'administration que pour les fournisseurs de services de coffre-fort numérique qui souhaiteraient bénéficier de cette certification. En effet, c'est l'administration et particulièrement l'ANSSI qui a la responsabilité de mettre en œuvre le schéma lié à la certification des services de coffre-fort numérique et, une fois ce schéma mis en œuvre, de procéder à la certification desdits services. Pour les fournisseurs de ces services, la certification représente un coût significatif lié à la mise en conformité aux exigences prévues par le cahier des charges mentionné par l'avant-dernier alinéa de l'article L. 103 du CPCE d'une part et un coût lié au processus de certification d'autre part.

*

* *

Article 26

Habilitation des agents de plusieurs organismes à rechercher et constater les manquements et infractions en matière de cybersécurité

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article permet aux agents de l'ANSSI, 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté plusieurs amendements qui ont :

– supprimé la référence aux infractions pouvant être commises par les personnes contrôlées par l'ANSSI compte tenu de la mise en place du régime d'amendes administratives ;

– clarifié le rôle des agents et personnels des organismes indépendants en matière de recherche des manquements, en limitant les interventions 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 ;

– apporté des modifications purement rédactionnelles ;

– précisé que les agents et personnels des organismes indépendants ou experts spécialement habilités par l'ANSSI peuvent concourir à la recherche des manquements mentionnés au premier alinéa de l'article sous le contrôle des agents et personnels mentionnés au même premier alinéa ;

– prévu la supervision de l'activité de certification par des organismes d'évaluation de la conformité en plus de l'ANSSI ;

– précisé que la recherche de manquements peut être effectuée par des experts qui ne seront ni des contrôleurs au sens du premier alinéa de l'article, ni des organismes indépendants.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté plusieurs amendements visant principalement à :

– tirer les conséquences de l'abrogation de la certification des services de coffre-fort numérique à l'article 26 A du projet de loi en supprimant corrélativement la compétence de l'ANSSI pour contrôler le respect de cette certification ;

– soumettre au contrôle de l'ANSSI les OIV qui ne sont pas déjà soumis à son contrôle en tant qu'entité essentielle ou importante ;

– appliquer le règlement UE n°2024/2847 dit CRA (Cyber Resilience Act) qui impose des exigences de cybersécurité aux fournisseurs de produits numériques accessibles sur le marché unique.

1. L'état du droit

Pour contrôler l'application des nouvelles obligations incombant aux entités contrôlées en matière de cybersécurité, l'ANSSI s'est vue attribuer des missions supplémentaires depuis sa création en 2009.

En premier lieu, pour l'application du 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 eIDAS, l'ANSSI assure un triple rôle :

– de certification, d'une part, de la conformité des moyens d'identification électronique aux exigences du cahier des charges, qu'elle établit, et d'autre part, de la délivrance d'une certification attestant du niveau de garantie aux prestataires fournissant un moyen d'identification électronique autre que présumé fiable ;

– de publication sur son site internet des décisions de certification en cours de validité ;

– et de contrôle, soit par ses propres moyens, soit par le biais d'un prestataire de confiance.

Par ailleurs, l'ANSSI est, en application du *Cyber Security Act* (CSA) de 2019, l'autorité nationale en matière de certification.

2. Le dispositif proposé

Le **premier alinéa** 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 eIDAS de 2014 (**alinéa 2**);

– le règlement CSA de 2019 (**alinéa 3**) ;

– les chapitres II et III du titre II du projet de loi, respectivement consacrés à la cyber-résilience et à la supervision (**alinéa 4**) ;

– les articles L. 100, L. 102 et L. 103 du code des postes et des communications électroniques (CPCE) relatifs aux envois recommandés électroniques et aux services de coffre-fort numérique (**alinéa 5**) ;

– les exigences de cybersécurité résultants des autorisations, certifications, qualifications et agréments que l'ANSSI délivre (**alinéa 6**).

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement des rapporteurs en commission qui a procédé à plusieurs modifications :

– il a supprimé la référence aux infractions pouvant être commises par les personnes contrôlées par l'ANSSI compte tenu de la mise en place du régime d'amendes administratives (**alinéa 1er**) ;

– il a clarifié le rôle des agents et personnels des organismes indépendants en matière de recherche des manquements, en limitant les interventions 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 (**alinéa 6**) ;

– il a apporté des modifications purement rédactionnelles (**alinéa 5**).

En outre, le Sénat a adopté un amendement à l'initiative du gouvernement en séance publique, qui a reçu un avis favorable de la commission, précisant la rédaction en :

– prévoyant la supervision de l'activité de certification par des organismes d'évaluation de la conformité en plus de l'ANSSI (**alinéa 6)** ;

– et en précisant que la recherche de manquements peut être effectuée par des experts (par exemple des expertises d'autorités de supervision d'États de l'Union européenne dans le cadre d'enquêtes transfrontalières, de consultants indépendants ou d'agents de l'État dont l'expertise pointue et temporaire pourrait être utile sans pour autant qu'il ne soit nécessaire de les désigner et de les faire assermenter) qui ne seront ni des contrôleurs au sens du premier alinéa de l'article, ni des organismes indépendants (**alinéa 7**).

4. La position de la commission

Outre un amendement rédactionnel de la rapporteure Anne Le Hénanff, la commission spéciale a adopté six amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff tirant les conséquences de l'abrogation de la certification des services de coffre-fort numérique à l'article 26 A du projet de loi en supprimant corrélativement la compétence de l'ANSSI pour contrôler le respect de cette certification ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff permettant de soumettre au contrôle de l'ANSSI les OIV qui ne sont pas déjà soumis à son contrôle en tant qu'entité essentielle ou importante. En effet, la rédaction initiale de l'article ne couvrait que les OIV des secteurs prévus par les directives NIS 2 et REC soumis au contrôle en vertu des chapitres II et III du projet de loi alors que les OIV hors du champ des directives relèvent uniquement de l'article L. 1332-11 du code de la défense portant les obligations qui leur sont applicables ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui ont pour objectif d'appliquer le règlement UE n°2024/2847 dit CRA (Cyber Resilience Act) visant à imposer des exigences de cybersécurité aux fournisseurs de produits numériques accessibles sur le marché unique, qui entrera prochainement en vigueur en droit national.

*

* *

Article 27

Droits et obligations des agents chargés d'un contrôle de l'ANSSI et de la personne contrôlée

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article oblige 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté deux amendements rédactionnels.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant à :

– introduire un critère de nécessité pour apprécier la légalité des demandes aux systèmes d'information, logiciels, programmes informatiques et données stockées appartenant aux entités contrôlées dans le cadre d'un contrôle diligenté par l'ANSSI ;

– supprimer la mention « *, qui doit comporter les questions auxquelles il est répondu* » de l'alinéa 6 ;

– compléter les prérogatives des agents en charge des contrôles des entités assujetties en ouvrant la possibilité de prélever des échantillons de produits.

1. L'état du droit

En application de l'article 8 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 opérateurs de services essentiels (OSE) peuvent être soumis par le premier ministre à des contrôles destinés à vérifier le respecte 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. Dans ce cadre, les OSE sont tenus de communiquer à l'ANSSI les informations et éléments nécessaires à la réalisation de ce contrôle.

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 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 euros d'amende en application de l'article 9 de la loi précitée. Ils encourent par ailleurs une amende de 125 000 euros s'ils font obstacle aux opérations de contrôle.

Par ailleurs, en vertu de l'article 22 de la 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, le premier ministre peut demander à l'ANSSI, à des services de l'État désignés par lui ou à des prestataires de service qualifiés 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.

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 euros après mise en demeure, en applications de l'article L. 1332-7 du code de la défense.

Néanmoins, qu'il s'agisse des OSE ou des OIV, il n'existe aucune disposition législative ou réglementaire qui détermine les prérogatives reconnues aux agents chargés d'effectuer ces contrôles, ni les obligations qui s'imposent à eux.

2. Le dispositif proposé

Le **premier alinéa** prévoit que la personne faisant l'objet d'un contrôle de l'ANSSI met à disposition des agents et personnels mentionnés à l'article 26 du projet de loi les moyens nécessaires pour vérifier sur pièces et sur place le respect des obligations mentionnées au même article 26.

Par ailleurs, ces agents et personnels ont accès aux locaux à usage professionnel des entités contrôlées et sont habilités à :

– exiger la communication de tout document nécessaire à l'accomplissement de leur mission, quel qu'en soit le support, et obtenir ou prendre copie de ces documents par tout moyen et sur tout support (**alinéa 2**) ;

– recueillir, sur convocation, sur place ou sur demande, tout renseignement ou toute justification nécessaire au contrôle (**alinéa 3**) ;

– accéder aux systèmes d'information, aux logiciels, aux programmes informatiques et aux données stockées et en demander la transcription (**alinéa 5**) ;

– procéder, sur convocation ou sur place, aux auditions des personnes susceptibles d'apporter des éléments utiles à leurs constatations. Ils en dressent procès-verbal, qui doit comporter les questions auxquelles il est répondu. Les personnes entendues procèdent elles-mêmes à sa lecture, peuvent y faire consigner leurs observations et y apposent leur signature. Si elles déclarent ne pas pouvoir lire, lecture leur en est faite préalablement à la signature. En cas de refus de signer le procès-verbal, mention en est faite sur celui-ci (**alinéa 6**).

En outre, dans le cadre du contrôle, le secret professionnel ne peut être opposé aux agents et personnels (**alinéa 7**). Toutefois, ces derniers sont tenus au secret professionnel pour les éléments dont ils ont connaissance en raison de leurs fonctions, sous réserve des éléments utiles à l'établissement des documents nécessaires à l'instruction (**alinéa 8**).

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 (**alinéa 9**).

Enfin, il est dressé procès-verbal des vérifications et visites menées dans le cadre du contrôle, qui fait foi jusqu'à preuve du contraire (**alinéa 10**).

3. Les modifications apportées par le Sénat

Le Sénat a adopté deux amendements rédactionnels.

Le premier amendement, adopté en commission à l'initiative des rapporteurs, apporte plusieurs modifications d'ordre légistique pour renforcer la sécurité juridique du dispositif, notamment en ce qui concerne les modalités d'établissement des procès-verbaux d'auditions.

Le second amendement, adopté en séance publique à l'initiative des rapporteurs avec un avis favorable de la commission, a apporté une modification d'ordre légistique à l'alinéa premier.

4. La position de la commission

La commission spéciale a adopté quatre amendements :

– deux amendements identiques de M. Denis Masséglia, de Mme Sabine Thillaye et de M. Laurent Mazaury qui introduisent un critère de nécessité pour apprécier la légalité des demandes aux systèmes d'information, logiciels, programmes informatiques et données stockées appartenant aux entités contrôlées dans le cadre d'un contrôle diligenté par l'ANSSI ;

– un amendement de la rapporteure Anne Le Hénanff qui supprime la mention « *, qui doit comporter les questions auxquelles il est répondu* » de l'alinéa 6. En effet, imposer lors d'un contrôle la rédaction des questions auxquelles les entités correspond dans les faits à une exigence prévue dans le cadre des procédures pénales et non en contrôle de nature administrative. Cette exigence est, en outre, source de complexité pour les contrôleurs et pour l'entité contrôlée au regard du déroulement pratique d'un contrôle en matière de système d'informations où les demandes et échanges se succèdent. L'entité peut faire des observations de procès-verbal ;

– et un amendement du rapporteur général Éric Bothorel, qui complète les prérogatives des agents et personnels en charge des contrôles des entités assujetties en ouvrant la possibilité de prélever des échantillons de produits.

*

* *

Article 28

Devoir de coopération de la personne contrôlée et amende administrative en cas d'obstacle à un contrôle

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article oblige les personnes contrôlées par l'ANSSI à coopérer avec elle et à instaurer une amende administrative prononcée en cas d'obstacle au contrôle.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement afin d'apporter des modifications de nature rédactionnelles et de préciser 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.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté plusieurs amendements visant principalement à distinguer le montant des sanctions en fonction de la qualification de l'entité : 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent pour les entités essentielles, et 7 millions d'euros ou 1,4 % du

chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent pour les entités importantes.

1. L'état du droit

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, dite directive NIS 2, prévoit que les États membres veillent à ce que les amendes administratives imposées aux entités essentielles et importantes pour des violations de la directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

Si un régime de sanctions pénales existe bien en vertu de l'article 9 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 transposant la directive dite NIS 1 pour les opérateurs de services essentiels (OSE) et de l'article L. 1332-7 du code de la défense pour les opérateurs d'importance vitale (OIV), ce régime de sanctions pénales n'a, dans les faits, jamais été appliqué.

Les paragraphes 2 et 3 de l'article 34 de la directive prévoient ainsi que les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, 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 ; les entités importantes sont 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.

2. Le dispositif proposé

Le **premier alinéa** transpose l'article 34 de la directive en obligeant les personnes contrôlées à coopérer avec l'ANSSI. Il habilite également 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.

En outre, le fait pour la personne contrôlée de faire obstacle aux contrôles, 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 L. 1332-15 du code de la défense, 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 appartient la personne contrôlée, le montant le plus élevé étant retenu (**alinéa 2**).

L'**alinéa 3** précise que l'ANSSI notifie à la personne contrôlée les griefs constitutifs d'obstacle retenus à son encontre et saisit la commission des sanctions.

Ces dispositions ne s'appliquent ni aux administrations de l'État, ni à ses établissements publics administratifs (**alinéa 4**). La directive permet en effet 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.

S'agissant du régime des sanctions, le Conseil d'État considère dans son avis que la possibilité ouverte par la directive d'aménager voire d'exempter les entités administratives des amendes administratives peut être mobilisée à l'égard des administrations de l'État et de ses établissements publics, dans la mesure où le gouvernement dispose à leur égard d'autres moyens que ces amendes pour garantir le respect de leurs obligations. Il estime en revanche qu'il n'en va pas de même des collectivités territoriales et de leurs groupements et établissements, en l'absence de dispositif d'effet équivalent et qu'en conséquence cette exemption ne peut être admise.

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement en commission à l'initiative des rapporteurs afin d'y apporter des modifications de nature rédactionnelles 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, conformément aux stipulations de la directive NIS 2.

4. La position de la commission

Outre un amendement rédactionnel de la rapporteure Anne Le Hénanff, la commission spéciale a adopté deux amendements identiques de M. Denis Masséglia et de Mme Marina Ferrari, qui distinguent le montant des sanctions en fonction de la qualification de l'entité : 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent pour les entités essentielles, et 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent pour les entités importantes.

*

* *

Article 29
Forme et prise en charge financière des contrôles

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit les formes que pourraient revêtir les contrôles de l'ANSSI et à en faire supporter le coût par la personne contrôlée.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement en commission pour prévoir que la personne 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.

Par ailleurs, le Sénat a adopté un amendement pour modifier les conditions dans lesquelles le coût des contrôles peut être mis à la charge de l'entité assujettie, dans le but d'éviter toute surtransposition.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant principalement à prévoir que les entités mentionnées à l'article 14 du projet de loi peuvent choisir les prestataires de services certifiés, qualifiés ou agréés ou organismes indépendants sur la base d'une liste élaborée par l'ANSSI.

1. L'état du droit

Les articles 32 et 33 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, dite directive NIS 2, prévoient que les autorités compétentes aient, dans le cadre de leur mission de supervision, le pouvoir de soumettre les entités essentielles (article 32) et importantes (article 33) à :

– des inspections sur place et des contrôles à distance ;

– des audits de sécurité réguliers et ciblés ;

– des scans de sécurité ;

– des demandes d'informations nécessaires à l'évaluation de la situation ;

– des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de leur mission de supervision ;

– et des demandes de preuves de la mise en œuvre des politiques de cybersécurité.

De plus, 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 par ailleurs que le coût d'un audit de sécurité ciblé effectué par un organisme indépendant doit être pris en charge par l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés. Aujourd'hui, la loi met déjà 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.

2. Le dispositif proposé

Le **premier alinéa** prévoit les différentes formes que pourra prendre un contrôle de l'ANSSI, à savoir :

– des inspections sur place et des contrôles à distance (**alinéa 2**) ;

– des audits de sécurité réguliers et ciblés réalisés par l'ANSSI ou par un organisme indépendant choisi par elle (**alinéa 3**) ;

– des scans de sécurité (**alinéa 5**) ;

– et des audits en cas d'incident important ou d'une violation des dispositions de l'article 26 (**alinéa 6**).

En outre, il était initialement prévu que le coût du contrôle soit pris en charge par la personne contrôlée, « *sauf, lorsque, à titre exceptionnel* », l'ANSSI en décidait autrement (**alinéa 7**).

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement en commission à l'initiative des rapporteurs pour prévoir que la personne 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. La commission a estimé

que le choix de faire reposer le coût de ces contrôles sur la personne contrôlée va bien au-delà des prescriptions de la directive, qui 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. À l'issue de ses travaux, les rapporteurs ont estimé qu'il était possible 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.

Par ailleurs, le Sénat a adopté en séance publique un amendement du gouvernement qui a reçu un avis favorable de la commission pour modifier les conditions dans lesquelles le coût des contrôles peut être mis à la charge de l'entité assujettie, dans le but d'éviter toute surtransposition. Le dispositif adopté prévoit que ne puissent être pris en charge par l'entité assujettie aux contrôles que les coûts résultant des audits de sécurité ciblés, conformément aux articles 32 et 33 de la directive NIS 2.

4. La position de la commission

Outre deux amendements rédactionnels de la rapporteure thématique, la commission a adopté un amendement de la rapporteure Anne Le Hénanff qui prévoit que les entités mentionnées à l'article 14 du projet de loi peuvent choisir les prestataires de services certifiés, qualifiés ou agréés ou organismes indépendants sur la base d'une liste élaborée par l'ANSSI. Cet amendement fait suite à de nombreuses inquiétudes soulevées lors des auditions, notamment s'agissant d'un potentiel risque confit d'intérêt entre l'audité et l'auditeur. Avec une liste de plusieurs prestataires établie par l'ANSSI, l'entité auditée ne sera pas contrainte de se faire auditer par un acteur directement concurrent par exemple.

*

* *

Article 30

Modalités d'application des dispositions relatives aux prérogatives de l'ANSSI en matière de recherche et de constatation des manquements

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article renvoie 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. Le dispositif proposé

Cet article prévoit que les modalités d'application de la section 1 « Recherche et constatations des manquements » du chapitre III du projet de loi sont fixées par décret en Conseil d'État.

2. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

3. La position de la commission

La commission spéciale n'a pas modifié cet article.

*

* *

Section 2
Mesures consécutives aux contrôles

Article 31
Ouverture d'une procédure à l'encontre de la personne contrôlée

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article permet à l'ANSSI d'ouvrir une procédure à l'encontre de la personne contrôlée au vu des résultats du contrôle.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a modifié cet article en introduisant les dispositions de l'article 32 du projet de loi dans le présent article 31 (*cf.* commentaire de l'article 32).

Par ailleurs, le Sénat a supprimé la possibilité pour l'ANSSI prévue à la fin de l'alinéa 9 de l'article 32 du projet de loi dans sa version initiale de rendre publique la mesure d'exécution adoptée et d'enjoindre à la personne contrôlée de rendre public son manquement.

En outre, le Sénat a modifié l'alinéa 1er de l'article pour permettre l'ouverture d'une procédure à l'encontre de l'entité contrôlée lorsque le contrôle mené révèle des éléments ou des faits éveillant une suspicion de manquement. Les agents chargés de l'instruction devront alors vérifier si le manquement peut ou non être qualifié et déterminer si l'adoption d'une mesure d'exécution est requise ou non dans les circonstances de l'espèce.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant à clarifier les suites à donner en cas de manquement ou de suspicion de manquement aux obligations prévues par le projet de loi et à préciser que les astreintes sont prononcées par l'ANSSI.

1. L'état du droit

En application de l'article 8 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 transposant la directive dite NIS 1, lorsqu'un manquement est constaté dans le cadre d'un contrôle d'un opérateur de services essentiels (OSE), l'ANSSI peut mettre en demeure les dirigeants de l'OSE concerné de se conformer aux obligations qui leur incombent dans un délai qu'elle détermine. Le fait, pour un OSE, de ne pas se conformer aux règles de sécurité qui s'imposent à lui à l'issue du délai fixé est puni de 100 000 euros d'amende, en application de l'article 9 de la loi susmentionnée.

S'agissant des OIV, l'article L. 1332-7 du code de la défense prévoit un régime similaire, l'amende étant portée à 150 000 euros les concernant.

Les articles 32 et 33 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, dite directive NIS 2, prévoient que les États membres veillent à ce que leurs autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécutions à l'égard d'entités essentielles (article 32) ou importantes (article 33), aient *a minima* le pouvoir :

– d'émettre des avertissements concernant les violations de la présente 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 présente 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 ou de respecter les obligations d'information énoncées à l'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 ;

– 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 présente 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.

S'agissant des entités essentielles, les autorités compétentes doivent également 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, si les mesures prises sont inefficaces, les États membres veillent à ce que leurs autorités compétentes aient le pouvoir de fixer un délai dans lequel l'entité essentielle est 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 veillent à ce que leurs autorités compétentes aient le pouvoir de suspendre temporairement ou de demander à un organisme de certification ou d'autorisation ou à une juridiction 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.

Enfin, les États membres peuvent imposer des astreintes pour contraindre les entités essentielles et importantes à mettre un terme à une violation de la directive conformément à une décision préalable de l'autorité compétente.

2. Le dispositif proposé

Le **premier alinéa** permet à l'ANSSI d'engager une procédure à l'encontre de la personne contrôlée au vu des résultats d'un contrôle en cas de constatation de manquements ou de suspicion de manquements aux obligations mentionnées à l'article 26. Dans ce cas, l'ANSSI notifie son intention à la personne contrôlée.

3. Les modifications apportées par le Sénat

Le Sénat a modifié cet article en commission à l'initiative des rapporteurs en introduisant les dispositions de l'article 32 du projet de loi dans le présent article 31 (*cf.* commentaire de l'article 32).

Les **alinéas 2 à 11** encadrent la manière dont se déroulerait la procédure ouverte par l'ANSSI à l'encontre de la personne contrôlée au vu des résultats d'un contrôle.

Si l'instruction ne fait pas état de faits justifiant une mesure d'exécution, l'ANSSI clôt la procédure et en informe la personne concernée. Dans le cas contraire, l'ANSSI est habilitée à adopter une mesure d'exécution après avoir mis

la personne concernée en mesure de présenter ses observations (**alinéa 4**). Elle pourrait ainsi :

– prononcer une mise en garde à l'encontre de la personne contrôlée (**alinéa 5)** ;

– 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 (**alinéa 6**) ;

– 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 (**alinéa 7**) ;

– lui ordonner d'informer les personnes 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 (**alinéa 8**) ;

– lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité (**alinéa 9**) ;

La mesure d'exécution pourrait être assortie d'une mesure d'astreinte dont le montant serait plafonné à 5 000 euros par jour de retard (**alinéa 10**).

L'**alinéa 11** organise les modalités de liquidation de l'astreinte.

Par ailleurs, cet amendement a supprimé la possibilité pour l'ANSSI prévue à la fin de l'alinéa 9 de l'article 32 du projet de loi dans sa version initiale de rendre publique la mesure d'exécution adoptée et d'enjoindre à la personne contrôlée de rendre public son manquement. Ainsi, seule la commission des sanctions serait habilitée à décider d'une mesure de publicité de la sanction.

En outre, le Sénat a modifié l'alinéa 1er de l'article en séance publique à l'initiative des rapporteurs pour permettre l'ouverture d'une procédure à l'encontre de l'entité contrôlée lorsque le contrôle mené, sans aboutir à la constatation d'un manquement évident de la part de cette entité, révèle des éléments ou des faits éveillant une suspicion de manquement. Les agents chargés de l'instruction devront alors vérifier si le manquement peut ou non être qualifié et déterminer si l'adoption d'une mesure d'exécution est requise ou non dans les circonstances de l'espèce.

4. La position de la commission

Outre un amendement de la rapporteure Anne Le Hénanff qui précise que les astreintes sont prononcées par l'ANSSI, la commission a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff de clarification sur les suites à donner en cas de manquement ou de suspicion de manquement aux obligations prévues par le projet de loi.

En effet, l'article 31 doit prévoir des conditions de déclenchement de la phase d'instruction, compatibles avec la réalité opérationnelle des contrôles. Or, si c'est effectivement le cas lorsque, de manière évidente, les mesures de contrôle ont révélé un manquement, cela doit également être possible lorsque le constat de certains faits sont susceptibles de révéler un manquement qui n'est pas encore qualifié ou pleinement établi au moment de l'ouverture de l'instruction. Dans certaines hypothèses, la qualification d'un manquement nécessitera des mesures d'instructions approfondies assorties de mesures de contrôle complémentaires, le cas échéant. Ainsi, la phase d'instruction permettra la qualification de certains faits au regard des règlementations mentionnées à l'article 26 du projet de loi justement pour déterminer si des manquements peuvent être identifiés.

*

* *

Article 32 (suppression maintenue)
Mesures d'exécution

Suppression maintenue par la Commission

➢ **Résumé du dispositif et effets principaux**

Cet article détermine 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement de suppression de l'article, dont le dispositif a été intégré à l'article 31 du projet de loi par souci de clarté et de lisibilité.

➢ **Modifications apportées par la commission**

Sans objet.

1. Le dispositif proposé

Dans sa rédaction initiale, cet article détaillait la manière se déroulerait la procédure ouverte par l'ANSSI à l'encontre de la personne contrôlée au vu des résultats d'un contrôle.

2. Les modifications apportées par le Sénat

Le Sénat a adopté en commission à l'initiative des rapporteurs un amendement de suppression de l'article, dont le dispositif a été intégré à l'article 31 du projet de loi par souci de clarté et de lisibilité.

3. La position de la commission

La commission a maintenu la suppression de cet article.

*

* *

Article 33
Saisine par l'ANSSI de la commission des sanctions

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit la saisine de l'ANSSI de la commission des sanctions en cas d'inexécution d'une mesure d'exécution.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement visant à améliorer la rédaction de l'article, à procéder aux coordinations découlant de l'intégration des dispositions de l'article 32 du 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.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant principalement à tirer les conséquences de précédents amendements qui excluent les personnes morales dont les activités sont visées à l'article L. 1332-2 du code de la défense du champ de la directive NIS 2 tout en garantissant leur assujettissement à un niveau d'exigence équivalent en soumettant ces personnes aux mesures consécutives à un contrôle prévues au présent article.

1. Le dispositif proposé

L'article 33 du projet de loi encadre les modalités de conclusion de 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.

Si l'ANSSI constate qu'il n'y a pas lieu de poursuivre la procédure au motif que la personne concernée a fourni les éléments montrant qu'elle s'est conformée à la mesure d'exécution dans le délai imparti, elle notifie sa décision à ladite personne (**premier alinéa**).

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 projet de loi (**alinéa 2**).

Dans le cas où la personne contrôlée serait une entité essentielle et où elle n'apporterait pas la preuve qu'elle s'est mise en conformité avec les mesures d'exécutions édictées par l'ANSSI dans le délai imparti, l'ANSSI pourrait suspendre une certification ou une autorisation concernant tout ou partie des services fournis ou des activités exercées par l'entité jusqu'à ce que celle-ci ait mis un terme au manquement (**alinéa 3**).

En outre, lorsque cette certification ou cette autorisation a été délivrée par un organisme de certification ou d'autorisation tiers, l'ANSSI pourrait enjoindre à cet organisme de la suspendre jusqu'à ce que l'entité ait mis un terme au manquement.

2. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement en commission à l'initiative des rapporteurs visant à améliorer la rédaction de l'article, à procéder aux coordinations découlant de l'intégration des dispositions de l'article 32 du 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.

3. La position de la commission

Outre un amendement rédactionnel de la rapporteure Anne Le Hénanff, la commission spéciale a adopté deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui tirent les conséquences de précédents amendements qui excluent les personnes morales dont les activités relèvent de l'article L. 1332-2 du code de la défense du champ de la directive NIS 2 tout en garantissant leur assujettissement à un niveau d'exigence équivalent en soumettant ces personnes aux mesures consécutives à un contrôle prévues au présent article.

Enfin, ces amendements simplifient la rédaction de l'alinéa 3 de l'article 33 en supprimant la mention des articles 8 à 10.

*

* *

Article 33 bis (nouveau)

Dématérialisation des actes établis par les agents et personnels compétents en matière de cybersécurité

Introduit par la Commission spéciale

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit la possibilité d'une procédure dématérialisée pour l'établissement ou la conversion des actes mentionnés dans le titre II du projet de loi. Ces actes sont établis par les agents et personnels mentionnés à l'article 26 du projet de loi.

Avec ce régime de dématérialisation, les actes peuvent être établis ou convertis sous format numérique et peuvent être intégralement conservés sous cette forme, dans des conditions sécurisées, sans nécessité de support papier. Lorsque ces actes sont établis sous format numérique et que les dispositions du présent titre exigent qu'ils soient signés, ils font l'objet, quel qu'en soit le nombre de pages et pour chaque signataire, d'une signature unique sous forme numérique, selon des modalités techniques qui garantissent que l'acte ne peut plus ensuite être modifié. Ces actes n'ont pas à être revêtus d'un sceau.

➢ **Dernières modifications législatives intervenues**

Sans objet.

1. L'état du droit

Sans objet.

2. Le dispositif introduit par la commission spéciale

Cet article additionnel a été introduit par l'adoption de deux amendements identiques du rapporteur général Éric Bothorel d'une part et de M. Thiébaut, M. Albertini, Mme Le Hénanff et Mme Saint-Paul d'autre part.

*
* *

Article 34
Modalités d'application des dispositions relatives à la procédure pouvant être engagée par l'ANSSI à l'encontre de la personne contrôlée

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article renvoie 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.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

➢ **Modifications apportées par la commission**

La commission a adopté un amendement rédactionnel.

1. Le dispositif proposé

L'article 34 prévoit la fixation par un décret en Conseil d'État des modalités d'application de la section 2 du chapitre III du 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 de ce contrôle.

2. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

3. La position de la commission

La commission spéciale a adopté un amendement rédactionnel de la rapporteure Anne Le Hénanff.

*
* *

Section 3
Des sanctions

Article 35
Compétence de la commission des sanctions

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

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 chapitres II « De la cyber-résilience » et III « De la supervision » du projet de loi.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement rédactionnel en commission.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

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 directive NIS 2, ne prévoit pas explicitement la mise en place d'une commission des sanctions. Il s'agit d'une initiative inscrite dans le projet de loi afin de garantir la bonne application des mesures prévues par la directive.

Elle se fonde toutefois sur les stipulations de l'article 36 de la directive qui prévoit que les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces

sanctions. Ainsi, la création de la commission des sanctions constitue une mesure nécessaire pour assurer la mise en œuvre des sanctions prévues par la directive.

2. Le dispositif proposé

La commission des sanctions, instituée auprès du premier ministre, est créée par l'article 1er du projet de loi, qui introduit un article L. 1332-15 dans le code de la défense à cette fin. L'article 35 du projet de loi prévoit que la commission des sanctions statue sur les manquements constatés aux obligations découlant de l'application des chapitres II et III du titre II du projet de loi, dans les conditions prévues par la section 3 du chapitre III du projet de loi.

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement rédactionnel en commission à l'initiative des rapporteurs précisant au début de l'alinéa premier que la commission des sanctions est saisie par l'ANSSI.

4. La position de la commission

La commission spéciale n'a pas modifié cet article.

*

* *

Article 36
Composition de la commission des sanctions

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit la composition de la commission des sanctions lorsqu'elle doit statuer sur l'application des chapitres II « De la cyber-résilience » et III « De la supervision » du projet de loi.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté plusieurs amendements à cet article visant à :

– préciser que la commission des sanctions est saisie par l'ANSSI ;

– prévoir que le premier ministre ne nommait qu'une des trois personnalités qualifiées, les deux autres étant nommées par les présidents des deux assemblées parlementaires ;

– préciser que les personnalités qualifiées membres de la commission des sanctions ne doivent pas avoir exercé de fonctions au sein de l'ANSSI depuis moins de cinq ans ;

– limiter la possibilité de nommer des personnalités qualifiées aux seules personnes qui n'ont pas exercé, au cours des trois années précédant leur nomination, une activité ni au sein de l'une des entités essentielles ou importantes mentionnées aux articles 8 et 9 du projet de loi, ni au sein de l'ANSSI.

➢ **Modifications apportées par la commission**

La commission a adopté plusieurs amendements qui visent à revenir sur le régime d'incompatibilité adopté par le Sénat consistant à exclure la nomination en tant que personne qualifiée au sein de la commission des sanctions de toute personne ayant exercé au cours des trois années précédentes une activité au sein de l'ANSSI ou au sein d'entités essentielles ou importantes.

1. L'état du droit

Comme indiqué dans le commentaire de l'article 35 du projet de loi, il n'existe pas actuellement de commission des sanctions dans le domaine de la cybersécurité. Celle-ci est créée par l'article 1er du projet de loi, en application des stipulations de l'article 36 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, dite directive NIS 2.

2. Le dispositif proposé

Le présent article prévoyait initialement que lorsque la commission des sanctions serait saisie par l'ANSSI, elle serait 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 de la commission des sanctions, 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 (**alinéa 2**) ;

– et de trois personnalités qualifiées, nommées par le premier ministre en raison de leurs compétences dans le domaine de la sécurité de systèmes d'information (**alinéa 3**).

La composition de la commission des sanctions est donc différente selon qu'elle soit saisie sur le fondement des dispositions du titre I^er^ ou du titre II du projet de loi. Si elle est toujours composée d'un membre du Conseil d'État, de la Cour de cassation et de la Cour des comptes, les trois personnalités qualifiées sont désignées en raison de leurs compétences dans le domaine de la sécurité :

– des activités d'importance vitale (titre I^er^) ;

– des systèmes d'information (titre II).

3. Les modifications apportées par le Sénat

Le Sénat a adopté quatre amendements à cet article.

En commission, un premier amendement des rapporteurs a été adopté, précisant que la commission des sanctions est saisie par l'ANSSI.

Par ailleurs, un deuxième amendement des rapporteurs a été adopté en commission qui précise que les trois personnalités qualifiées sont nommées respectivement par le Premier ministre, le président de l'Assemblée nationale et le président du Sénat. Ainsi, alors que le premier ministre nommait les trois personnalités qualifiées dans la version initiale du projet de loi, le Sénat a prévu que celui-ci ne nommait qu'une des trois personnalités qualifiées, les deux autres étant nommées par les présidents des deux assemblées parlementaires.

Enfin, un troisième amendement des rapporteurs a été adopté en commission, qui précise que les personnalités qualifiées membres de la commission des sanctions ne doivent pas avoir exercé de fonctions au sein de l'ANSSI depuis moins de cinq ans. L'objectif poursuivi était de prévenir les conflits d'intérêts.

En séance publique, un amendement du gouvernement qui a reçu un avis favorable de la commission a été adopté, qui a limité la possibilité de nommer des personnalités qualifiées aux seules personnes qui n'ont pas exercé, au cours des trois années précédant leur nomination, une activité ni au sein de l'une des entités essentielles ou importantes mentionnées aux articles 8 et 9 du projet de loi, ni au sein de l'ANSSI. L'objectif poursuivi était là encore de prévenir les conflits d'intérêt.

4. La position de la commission

La commission a adopté trois amendements identiques du rapporteur général Éric Bothorel, de la rapporteure Anne Le Hénanff et de Mme Marina Ferrari qui visent à revenir sur le régime d'incompatibilité adopté par le Sénat consistant à exclure la nomination en tant que personne qualifiée au sein de la commission des sanctions de toute personne ayant exercé au cours des trois années précédentes une activité au sein de l'ANSSI ou au sein d'entités essentielles ou importantes. Cette incompatibilité ne permettrait en effet pas à la commission des sanctions de disposer de personnalités qualifiées sur les questions de cybersécurité.

*
* *

Article 37
Sanctions en cas de manquements aux obligations en matière de cybersécurité

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article transpose les différentes sanctions administratives prévues par la directive dite NIS 2 en cas de méconnaissance des obligations qu'elle impose aux entités régulées.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a apporté plusieurs modifications à cet article visant à :

– restreindre au V la faculté pour la commission des sanctions d'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 en indiquant que cette possibilité devait être envisagée en dernier recours et si le manquement persiste après que l'amende administrative a été prononcée ;

– prévoir que la commission des sanctions peut exiger que l'entité qui s'est rendue coupable d'un manquement communique au public, par tout moyen adapté et à ses frais, le manquement constaté (alinéa 14). La commission des sanctions peut d'ailleurs elle-même décider de rendre publique tout ou partie de sa décision si elle estime que cela va dans l'intérêt du public (alinéa 15) ;

– préciser que la commission des sanctions devait prendre en compte les circonstances et la gravité du manquement, le comportement de son auteur, notamment sa bonne foi, ainsi que ses ressources et ses charges lorsqu'elle fait le choix de sanctionner une entité qui s'est rendue coupable d'un manquement (alinéa 16).

➢ **Modifications apportées par la commission**

La commission spéciale a adopté plusieurs amendements visant principalement à :

– tirer les conséquences d'amendements précédents, en soumettant les personnes morales dont les activités sont visées à l'article L. 1332-2 du code de la défense au dispositif de sanction prévu au présent article ;

– appliquer le règlement CRA visant à imposer des objectifs de cybersécurité aux fournisseurs de produits numériques accessibles sur le marché unique, qui entrera prochainement en vigueur en droit national ;

– conditionner l'interdiction d'exercer des dirigeants des entités essentielles à l'inefficacité des mesures de police administrative mentionnées aux articles 25 et 31 du projet de loi.

1. L'état du droit

L'article 36 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, dite directive NIS 2, prévoit que les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à cette directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Il précise également que les sanctions prévues sont effectives, proportionnées et dissuasives.

Cette mention figure également à l'article 34 de la directive, qui stipule que les États membres veillent à ce que les amendes administratives imposées aux entités essentielles et importantes pour des violations de la directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas. Ce même article définit le montant des amendes encourues par les entités essentielles et importantes. Il précise également 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.

2. Le dispositif proposé

Le **I** du présent article établit les sanctions que la commission des sanctions peut prononcer à l'encontre des entités essentielles, des entités importantes, des offices d'enregistrement et des bureaux d'enregistrement.

S'agissant des entités essentielles et des opérateurs mentionnés à l'article L. 1332-2 du code de la défense, le montant de l'amende administrative ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial (**alinéa 2**).

S'agissant des entités importantes, le montant de l'amende administrative ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial (**alinéa 3**).

Les administrations de l'État et de ses établissements publics administratifs (EPA), des collectivités territoriales, de leurs groupements et de leurs

établissements publics administratifs ne peuvent se voir appliquer les sanctions mentionnées aux alinéas 2 et 3.

S'agissant des offices d'enregistrement et des bureaux d'enregistrement, le montant de l'amende administrative ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial. 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 (**alinéa 4**).

Il s'agit dans l'ensemble d'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. Toutefois, ainsi que l'a souligné le Conseil d'État, dans son avis sur le présent projet de loi, cette exemption soulève une difficulté d'ordre constitutionnel. Dans son avis, le Conseil d'État indique que l'exclusion des collectivités territoriales, de leurs groupements et de leurs EPA du champ des entités susceptibles de faire l'objet d'amendes administratives en cas de manquement aux obligations mises à leur charge ne se justifie pas compte tenu de l'objectif poursuivi par le projet de loi, à savoir de faire en sorte que la sécurité et la continuité des activités d'importance vitale pour le pays soient assurées, quel que soit le statut de l'opérateur qui les exerce. Il cite l'exemple de la fourniture d'eau potable, qui peut être assurée par des collectivités territoriales en régie. Le Conseil d'État considère en outre qu'une telle exemption ne serait pas compatible avec les termes de la directive et que, de ce fait, celle-ci méconnaît le principe d'égalité et les objectifs de la directive.

En outre, si les manquements constatés constituent également une violation du règlement général sur la protection des données (RGPD) et ont donné lieu à une amende de la CNIL, la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative (**alinéa 5**). Cette disposition constitue une application du principe *non bis in idem* au terme duquel nul ne peut être poursuivi ou puni pénalement à raison des mêmes faits.

Par ailleurs, le **II** du présent article prévoit que la commission des sanctions peut prononcer une amende administrative dont le montant ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial 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 que l'autorité nationale de sécurité des systèmes d'information certifie[1] et des organismes d'évaluation de la conformité, à l'exception des administrations de l'État et de leurs établissements

---

[1] *Comme le précise l'étude d'impact du projet de loi, au titre du règlement eIDAS de 2014, qui instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique et encadre en particulier la signature électronique, plusieurs rôles sont confiés à l'ANSSI : contrôler les prestataires de confiance, certifier les dispositifs de création de signature et de cachets électroniques qualifiés et établir, tenir à jour et publier la liste nationale des prestataires de services de confiance.*

publics à caractère administratif, en cas de manquement constaté 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 (**alinéa 7)** ;

– et 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 et de cybersécurité, des titulaires d'un agrément, d'une qualification ou d'un certificat dans le domaine de la cybersécurité, en cas de manquement constaté au règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA ou aux exigences mentionnées aux 4° et 5° de l'article 26 de la présente loi (**alinéa 8**).

Le **III** prévoit que lorsque la commission des sanctions envisage de prononcer l'amende prévue à l'article 28 du projet de loi à l'encontre de la même personne, le montant cumulé ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial (**alinéa 9**).

Le **IV** prévoit en outre que la commission des sanctions peut 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 :

– l'abrogation d'un agrément, d'une qualification ou d'un certificat (**alinéa 11**) ;

– et l'abrogation de l'autorisation, de l'agrément ou de l'habilitation délivrés à l'organisme d'évaluation de la conformité, lorsque le manquement n'est pas corrigé dans le délai imparti par l'ANSSI (**alinéa 12**).

Enfin, le **V** prévoit 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 b) du paragraphe 5 de l'article 32 de la directive NIS 2. Ces dispositions ne s'appliquent toutefois pas aux administrations (**alinéa 13**).

3. Les modifications apportées par le Sénat

Le Sénat a apporté plusieurs modifications à cet article.

Tout d'abord, un premier amendement adopté en commission à l'initiative des rapporteurs a restreint au **V** la faculté pour la commission des sanctions d'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 en indiquant que cette

possibilité devait être envisagée en dernier recours et si le manquement persiste après que l'amende administrative a été prononcée.

Par ailleurs, un second amendement des rapporteurs adopté en commission a introduit un **VI** prévoyant que la commission des sanctions peut exiger que l'entité qui s'est rendue coupable d'un manquement communique au public, par tout moyen adapté et à ses frais, le manquement constaté (**alinéa 14**). La commission des sanctions peut d'ailleurs elle-même décider de rendre publique tout ou partie de sa décision si elle estime que cela va dans l'intérêt du public (**alinéa 15**).

En séance publique, trois amendements identiques ont été adoptés, à l'initiative de Mmes Morin-Desailly et Conway-Mouret et de M. Bleunven, créant un **VII** précisant que la commission des sanctions devait prendre en compte les circonstances et la gravité du manquement, le comportement de son auteur, notamment sa bonne foi, ainsi que ses ressources et ses charges lorsqu'elle fait le choix de sanctionner une entité qui s'est rendue coupable d'un manquement (**alinéa 16**).

4. La position de la commission

Outre deux amendements rédactionnels de la rapporteure Anne Le Hénanff, la commission spéciale a adopté huit amendements :

– plusieurs amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui tirent les conséquences d'amendements précédents, en soumettant les personnes morales dont les activités sont visées à l'article L. 1332-2 du code de la défense au dispositif de sanction prévu à l'article 37 de la présente loi ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui appliquent le règlement CRA visant à imposer des objectifs de cybersécurité aux fournisseurs de produits numériques accessibles sur le marché unique, qui entrera prochainement en vigueur en droit national ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff qui conditionnent l'interdiction d'exercer des dirigeants des entités essentielles à l'inefficacité des mesures de police administrative (mesures d'exécution) mentionnées aux articles 25 et 31 du projet de loi, conformément aux articles 32 et 34 de la directive NIS 2.

*

* *

Article 37 bis (nouveau)

Octroi par l'ANSSI aux organismes d'évaluation du pouvoir d'évaluation de la conformité à des exigences de cybersécurité et à la délivrance de certificats de conformité

Introduit par la Commission spéciale

➢ **Résumé du dispositif et effets principaux**

Cet article donne une base législative pour permettre à l'ANSSI :

– d'une part, de confier au cas par cas dans les schémas de certification, l'activité de certification à des organismes d'évaluation de la conformité, soit en application du droit de l'Union, en particulier l'article 56.6 du règlement n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, soit pour la certification nationale, par exemple dans le cadre du décret n° 2010-112 du 2 février 2010 en application du référentiel général de sécurité ;

– et d'autre part, de soumettre à autorisation préalable ces organismes dans les cas où les schémas de certification européens ou nationaux le prévoient, afin d'évaluer leur aptitude à procéder à des évaluations et à la certification de la cybersécurité dans des domaines sensibles et présentant une technicité particulière, par exemple pour la qualification *SecNumCloud*.

➢ **Dernières modifications législatives intervenues**

Sans objet.

1. L'état du droit

Sans objet.

2. Le dispositif introduit par la commission spéciale

Cet article additionnel a été introduit par l'adoption de deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff.

*

* *

CHAPITRE IV
Dispositions diverses d'adaptation

Article 38
(art. 30 et 35 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)
Alléger le contrôle des biens de cryptologie

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article allège 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.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat n'a pas modifié cet article.

- **Modifications apportées par la commission**

La commission a adopté des amendements qui visent à améliorer la lisibilité du dispositif de déclaration des moyens de cryptologie pour les destinataires de l'obligation en permettant de s'appuyer sur le niveau règlementaire pour tenir à jour de manière régulière, en conformité avec les engagements européens en la matière, la liste des moyens et prestations concernés par l'obligation et éviter des formalités inutiles aux entreprises.

1. L'état du droit

Le titre III de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dite LCEN, est consacré à la sécurité dans l'économie numérique. Le chapitre I^{er} du titre III a trait aux moyens et prestations de cryptologie.

Aux termes du premier alinéa de l'article 29 de la loi LCEN, un moyen de cryptologie correspond à 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.

En outre, le deuxième alinéa de l'article 29 dispose que l'on entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie.

Par ailleurs, l'article 30 de la loi LCEN dispose que l'utilisation des moyens de cryptologie est libre. 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 libres.

De plus, 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, sauf dans des cas spécifiques.

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.

En outre, 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 soumis à autorisation du Premier ministre, sauf dans des cas spécifiques. 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 ;

– et 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 au III, soit dispensés de toute formalité préalable.

Le 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'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 mais sujets au risque de détournement d'usage à des fins militaires prohibées ou de prolifération nucléaire, biologique ou chimique, dont l'exportation est contrôlée. De ce fait, certains moyens de cryptologie sont également soumis à cette réglementation des BDU. Lorsqu'un BDU intègre un dispositif de cryptologie, une autorisation préalable d'exportation de bien de cryptologie délivrée par l'ANSSI est nécessaire, puis une autorisation de licence d'exportation de BDU délivrée par la commission interministérielle des biens à double usage (CIBDU), qui dépend du secrétariat général de la défense et de la sécurité nationale (SGDSN).

À ses articles 32 et 33, la loi LCEN définit également un principe de responsabilité civile pour les prestataires de services de cryptologie au titre des prestations fournies.

Elle définit, à son article 34, les sanctions administratives associées au non-respect de l'article 30 et, à son article 35, les sanctions pénales associées au non-respect des articles 30, 31 et 34.

2. Le dispositif proposé

L'objectif poursuivi par l'article est d'alléger la charge pour les entreprises et l'administration.

Le **1°** du présent article (**alinéa 2 à 8**) procède à une réécriture en profondeur de l'article 30 de la loi LCEN

Le I de l'article 30 demeure inchangé et prévoit toujours que l'utilisation des moyens de cryptologie est libre.

Au II de l'article 30, la seule modification opérée est la substitution de la mention « Communauté européenne » par la mention « Union européenne ».

Le III prévoit désormais 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 BDU intégrant un moyen de cryptologie.

Cette disposition fait donc passer d'un régime d'autorisation à un régime de déclaration préalable l'exportation de moyens de cryptologie. Cette évolution s'inscrit dans un objectif de simplification, notamment vis-à-vis de l'administration qui voit ainsi sa charge diminuée tout en maintenant un dispositif de contrôle et de recueil d'informations techniques sur les moyens de cryptologie.

En outre, l'obligation 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 source des logiciels utilisés, est retirée.

De plus, les dispositions du III ainsi modifié s'appliquent sans préjudice des exigences applicables aux BDU intégrant un moyen de cryptologie.

En conséquence le IV, qui prévoyait le régime d'autorisation, est abrogé.

Par ailleurs, le **2°** de l'article (**alinéa 8**) abroge l'article 33 de la loi LCEN, devenu obsolète. Cet article 33 prévoyait un régime de responsabilité civile des prestataires de services de certification électronique. Or, 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. L'abrogation de l'article 33 constitue donc une mesure de simplification et de clarification juridique.

Enfin, le **3°** de l'article (**alinéas 10 et 11**) réécrit le I de l'article 35 de la loi LCEN en punissant d'une peine d'an de prison et de 15 000 euros d'amende le fait de ne pas satisfaire à l'obligation prévue à l'article 30 de ladite 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. Cette modification a pour effet de faire disparaître 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 autorisation préalable lorsqu'une telle autorisation est exigée.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission a adopté deux amendements identiques du rapporteur général et de la rapporteure Anne Le Hénanff qui visent à améliorer la lisibilité du dispositif de déclaration des moyens de cryptologie pour les destinataires de l'obligation en permettant de s'appuyer sur le niveau règlementaire pour tenir à jour de manière régulière, en conformité avec les engagements européens en la matière, la liste des moyens et prestations concernés par l'obligation et éviter des formalités inutiles aux entreprises.

*
* *

Article 39

(art. L. 2321-2-1 et L. 2321-3 du code de la défense, art. L. 33-1, L. 45, L. 45-3, L. 45-4, L. 45-5 et L. 45-8 du code des postes et des communications électroniques, titre Ier de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité [supprimés], art. 1er, 9, 12 et 14 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives)

Abrogation de la transposition de la directive NIS 1 et simplification du cadre réglementaire

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article abroge la transposition de la directive dite 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.

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement rédactionnel.

- **Modifications apportées par la commission**

La commission a adopté plusieurs amendements visant à :

– définir les agents agissant pour le compte des bureaux d'enregistrement ;

– tenir compte de l'abrogation des articles 9 et 12 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.

1. L'état du droit

La transposition 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, dite directive

NIS 2, rend caduques toute une série de dispositions législatives. Parmi les dispositions législatives concernées, figurent :

– le titre Ier de la loi n° 2018-133 du 26 février 2018, qui assure la transposition en droit français de la directive dite NIS 1 ;

– 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 ;

– et les dispositions du code des postes et des communications électroniques (CPCE) portant sur les opérateurs de communication électronique et les offices d'enregistrement.

2. Le dispositif proposé

L'article 44 de la directive NIS 2 abrogeant la directive NIS 1, le **III** du présent article abroge le titre Ier de la loi n° 2018-133 du 26 février 2018, qui assure la transposition en droit français de cette directive.

En conséquence, les **alinéas 3, 4, 6** et **7** procèdent au remplacement de la référence à la loi du 26 février 2018 par la référence à la présente loi à différents articles du code de la défense. De même, en vertu de la directive NIS 2, les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE) mentionnés aux articles L. 2321-2-1 et L. 2321-3 du code de la défense sont remplacés par la notion d'entité essentielle.

Par ailleurs, le **II** du présent article apporte des modifications à plusieurs articles du CPCE relatifs aux modalités d'enregistrement des noms de domaine de premier niveau afin :

– 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 (**alinéa 10**) ;

– de modifier l'article L. 33-1 du CPCE en prévoyant 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 (**alinéas 11 à 15**)

– que chaque office d'enregistrement soit responsable du fonctionnement technique du domaine de premier niveau qui lui est attribué (**alinéa 17**) ;

– d'apporter une précision rédactionnelle à l'article L. 45-3 relatif à la numérotation et à l'adressage des noms de domaines (**alinéa 18**) ;

– d'ajouter des références aux agents agissant pour le compte des bureaux d'enregistrement à l'article L. 45-4 du CPCE (**alinéa 22**) et de prévoir qu'un décret en Conseil d'État vienne préciser les catégories auxquelles appartiennent lesdits agents (**alinéa 24**) ;

– que les offices d'enregistrement collectent les données nécessaires à l'enregistrement des noms de domaines (**alinéa 27**) ;

– et que les offices et les bureaux d'enregistrement répondent aux demandes d'accès aux données d'enregistrement dans un délai n'excédant pas 72 heures après réception de la demande (**alinéa 30**).

Enfin, le **IV** du présent article 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 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.

3. Les modifications apportées par le Sénat

Un amendement rédactionnel a été adopté en commission à l'initiative des rapporteurs.

4. La position de la commission

Outre trois amendements rédactionnels du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff, la commission spéciale a adopté quatre amendements :

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff visant à définir les agents agissant pour le compte des bureaux d'enregistrement. Ils prévoient également la reprise à l'article L. 45-5 du CPCE de la formulation retenue à l'article 22 du projet de loi afin de préciser que les offices et les bureaux d'enregistrement mentionnés dans le CPCE doivent répondre aux demandes des agents habilités à cet effet ;

– deux amendements identiques du rapporteur général Éric Bothorel et de la rapporteure Anne Le Hénanff de coordination pour tenir compte de l'abrogation des articles 9 et 12 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 par l'article 39 du projet de loi.

*

* *

Article 40

(art. 57 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, art. 24 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, art. 16 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives)

Mesures applicables à l'outre-mer pour les territoires régis par le principe de spécialité législative

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article étend l'application du titre II du projet de loi aux collectivités d'outre-mer par le régime de spécialité législative.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement en commission pour clarifier l'applicabilité en Nouvelle-Calédonie et en Polynésie française des modifications prévues à l'article 39 du projet de loi.

➢ **Modifications apportées par la commission**

La commission a adopté trois amendements rédactionnels.

1. L'état du droit

Si les dispositions 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, qui transposait la directive dite NIS 1, étaient directement applicables aux collectivités régies par le régime de l'identité législative, il avait fallu adopter des mesures spécifiques pour les collectivités régies par le régime de spécialité législative.

2. Le dispositif proposé

Les stipulations 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, dite NIS 2, sont applicables de plein droit aux collectivités d'outre-mer régies par le régime de l'identité législative, à savoir :

– les départements et régions de la Guadeloupe et de La Réunion ;

– les collectivités de la Guyane, de la Martinique et de Mayotte ;

– et Saint-Martin.

En outre, le **I** de l'article 40 prévoit que le titre II du projet de loi est applicable dans les collectivités régies par le principe de spécialité législative, à l'exception de l'article 13 du projet de loi, qui sont les suivantes :

– les îles Wallis et Futuna ;

– la Polynésie française ;

– la Nouvelle-Calédonie ;

– et les Terres australes et antarctiques françaises.

Cette application aux collectivités régies par le principe de spécialité législative se fait toutefois 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 (**alinéa 2**) ;

– dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie (**alinéas 3 et 4**).

Le **II** prévoit également que l'article 13 du présent projet de loi ne s'applique pas à Saint-Barthélemy et à Saint-Pierre-et-Miquelon (**alinéa 5**).

Le **III** dispose toutefois que sont applicables 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 dispositions du titre II du projet de loi « *en tant que droit national faisant référence au droit dérivé* ». Ainsi, dans ces territoires, les références à la directive NIS 2 et à d'autres textes européens sont remplacées par la référence aux règles en vigueur en métropole (**alinéa 6**).

Enfin, les **IV** à **VI** visent à coordonner les textes et à assurer la cohérence pour 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, et 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.

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement en commission à l'initiative des rapporteurs pour 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 prévus à l'article 39 du projet de loi. Il précise en particulier que le titre II s'applique en Nouvelle-Calédonie et en Polynésie française à l'exception des modifications des articles L. 45 et suivants du CPCE prévues par l'article 39 du projet de loi.

4. La position de la commission

La commission a adopté trois amendements rédactionnels de la rapporteure Anne Le Hénanff.

*

* *

CHAPITRE V
Dispositions relatives aux communications électroniques

Article 41
(art. L. 39-1 du code des postes et des communications électroniques)
Renforcement des sanctions pénales pour améliorer la lutte contre les brouillages

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article procède à une réécriture de l'article L. 39-1 du CPCE dans le sens d'un durcissement des sanctions pénales associées à certaines infractions.

– passage de six mois de prison et 30 000 euros d'amende à trois ans de prison et 75 000 euros d'amende pour les infractions de perturbation d'émissions hertziennes autorisées du fait de l'utilisation d'installations ou d'équipements électriques, électroniques et radioélectriques dans des conditions non conformes aux exigences essentielles des réglementations relatives à leurs mises sur le marché ou de l'utilisation de fréquences sans autorisation d'utilisation de fréquence ou de certificat d'opérateur ;

– passage de six mois de prison et 30 000 euros d'amende à cinq ans de prison et 150 000 euros d'amende pour le fait de pratiquer l'une des activités prohibées à l'article L. 33-3-1 du CPCE, à savoir importation, publicité, cession à titre gratuit

ou onéreux, mise en circulation, installation, détention et utilisation de tout dispositif destiné à rendre inopérants des appareils de communications électroniques de tous types. Il s'agit de ce qu'on appelle plus communément des brouilleurs ;

– et passage de six mois de prison et 30 000 euros d'amende à cinq ans de prison et 150 000 euros d'amende pour l'utilisation sans l'autorisation prévue à l'article L. 41-1 des fréquences ou des installations radioélectriques.

➢ **Dernières modifications législatives intervenues**

Sans objet.

➢ **Modifications apportées par le Sénat**

Deux amendements ont été adoptés par le Sénat. Un amendement rédactionnel a été adopté en commission mais le Sénat est revenu à la rédaction initiale lors de la séance publique.

➢ **Modifications apportées par la commission**

La commission a adopté six amendements rédactionnels.

1. L'état du droit

La transmission hertzienne, c'est-à-dire sur des liaisons sans fil (réseaux de téléphonie mobile, réseaux professionnels privés, WiFi…) de données ou de la voix tient une place essentielle dans la continuité des activités économiques, sociétales et étatiques. L'utilisation d'un appareil électrique, radioélectrique ou électronique ou d'une fréquence radioélectrique dans des conditions non conformes ou 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.

Ces dernières années, le nombre de cas de brouillage a connu une forte augmentation. Entre 1 400 et 1 800 cas sont signalés chaque année à l'Agence nationale des fréquences (ANFR), qui indique que ces brouillages peuvent avoir des conséquences de plus en plus graves en raison de l'évolution des technologies hertziennes et de la densification des usages dans des bandes de fréquences en partage avec d'autres services. Au-delà des brouillages accidentels, la préoccupation majeure porte sur l'utilisation délibérée de brouilleurs alors que la loi les prohibe pourtant. Ces outils sont d'une dangerosité particulièrement accrue, dans la mesure où ils peuvent, par exemple, perturber des avions volant à plus de 2 000 mètres d'altitude. Ces brouilleurs sont, du reste, de plus en plus souvent utilisés par des personnes qui souhaitent commettre des infractions et pourraient même constituer des outils de guerre électronique.

Dès lors, la lutte contre ces perturbations ou brouillages est une nécessité pour assurer le bon fonctionnement des services de communication par radiofréquence. Afin de dissuader les auteurs de brouillages, intentionnels ou non, l'article L. 39-1 du code des postes et des communications électroniques (CPCE) dispose qu'est puni de 6 mois de prison 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 ;

– de perturber, en utilisant une fréquence, un équipement ou une installation radioélectrique, dans des conditions non conformes ou sans posséder d'autorisation ou en dehors des conditions de cette autorisation ou des conditions réglementaires générales les émissions hertziennes d'un service autorisé ;

– 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, les émissions hertziennes d'un service autorisé ;

– d'utiliser une fréquence, un équipement ou une installation radioélectrique dans des conditions non conformes ou sans posséder d'autorisation ou en dehors des conditions de l'autorisation ou sans posséder le certificat d'opérateur ou en dehors des conditions réglementaires générales ou sans l'accord mentionné au I de l'article L. 43 ;

– et d'avoir pratiqué l'une des activités prohibées par le I de l'article L. 33-3-1 en dehors des cas et conditions prévus au II de cet article.

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.

La sanction maximale prévue par l'article L. 39-1 du CPCE est considérée comme faible dans le quantum des peines. Par ailleurs, non seulement les infractions constatées ne donnent que très rarement lieu à des poursuites, mais au demeurant, les peines prononcées sont souvent minimes. Comme l'indique le Sénat dans son rapport, 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.

2. Le dispositif proposé

Le présent article procède à une réécriture de l'article L. 39-1 du CPCE dans le sens d'un durcissement des sanctions pénales associées à certaines infractions.

● Un quantum de peine inchangé pour les infractions les moins graves

Le **deuxième alinéa** 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 (**alinéa 3**) ;

– d'utiliser une fréquence, un équipement ou une installation radioélectrique dans des conditions non conformes (**alinéa 5**), sans posséder l'autorisation (**alinéa 6**) ou en dehors des conditions de cette autorisation lorsque celle-ci est requise (**alinéa 7**), sans posséder le certificat d'opérateur (**alinéa 8**) ou en dehors des conditions réglementaires générales (**alinéa 9**).

Une nouvelle infraction est également créée, à l'**alinéa 10**, 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.

● Une sanction durcie en cas de perturbation des émissions hertziennes d'un service autorisé

L'alinéa 11 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 (**alinéa 13**), sans posséder l'autorisation (**alinéa 14**) ou en dehors des conditions de cette autorisation lorsque celle-ci est requise (**alinéa 15**), sans posséder le certificat d'opérateur (**alinéa 16**) ou en dehors des conditions réglementaires générales (**alinéa 17**), 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 (**alinéa 18**).

L'alinéa 19 prévoit également 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 un appareil, un équipement ou une installation, électrique ou électronique, dans des conditions non conformes à la réglementation régissant la compatibilité électromagnétique des équipements électriques et électroniques.

● Cinq ans de prison pour les cas de brouillages volontaires ou offensifs

L'**alinéa 20** prévoit qu'est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende le fait :

– d'avoir pratiqué 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 » (**alinéa 21**) ;

– d'utiliser, sans l'autorisation 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 attribuée par l'ANFR (**alinéa 22**).

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.

3. Les modifications apportées par le Sénat

Deux amendements ont été adoptés par le Sénat.

Le premier amendement, adopté en commission à l'initiative des rapporteurs, de nature rédactionnelle, a remplacé les mots « sous réserve » par les mots « sans préjudice » à l'alinéa 11 de l'article.

Le second amendement, adopté en séance publique à l'initiative gouvernement avec un avis favorable de la commission, a rétabli la rédaction initiale de l'alinéa 11 modifiée en commission en remplaçant les mots « sans préjudice » par les mots « sous réserve ».

Le gouvernement a justifié la nécessité de revenir à la rédaction initiale du projet de loi telle qu'issue du Conseil d'État par le fait que la substitution de la mention « sous réserve » par la mention « sans préjudice » aurait pour conséquence que l'administration devra choisir sur quel fondement elle entend sanctionner un brouillage alors que le quantum des peines diffère selon le fondement retenu.

4. La position de la commission

La commission a adopté six amendements rédactionnels de la rapporteure Anne Le Hénanff.

*

* *

Article 42

(art. L. 97-2 et L. 97-4 du code des postes et des communications électroniques)

Renforcement des conditions d'accès à une assignation de fréquences déposée par la France auprès de l'UIT

Adopté par la Commission avec modifications

- **Résumé du dispositif et effets principaux**

Cet article renforce les conditions d'accès à une assignation de fréquences déposée par la France auprès de l'Union internationale des télécommunications (UIT).

- **Dernières modifications législatives intervenues**

Sans objet.

- **Modifications apportées par le Sénat**

Le Sénat a adopté un amendement rédactionnel.

- **Modifications apportées par la commission**

La commission a adopté cinq amendements rédactionnels.

1. L'état du droit

Afin de délivrer un service, les systèmes satellitaires orbitaux doivent pouvoir communiquer avec des équipements placés sur terre. L'établissement d'un tel lien de communication est essentiel à l'activité de ces derniers, car il leur permet d'être commandés à distance et de transmettre des données (imagerie, télécommunication, *etc.*). Cette communication est établie grâce à l'émission et 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 permettant de communiquer entre les satellites géostationnaires et non géostationnaires et les stations terriennes constituent une ressource rare. 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. Afin d'en garantir la disponibilité et éviter ainsi les risques de brouillage entre satellites, l'UIT met en œuvre un processus préalable à tout lancement de satellites de déclaration des fréquences associées.

En pratique, il revient aux États de déposer auprès de l'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 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. En outre, l'article L. 97-2 du CPCE prévoit que toute demande d'assignation de fréquence relative à un système satellitaire est adressée à l'ANFR. 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 utilisant l'assignation de fréquence.

Toutefois, le I de l'article L. 97-2 prévoit que 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'UIT ;

– ou lorsque le demandeur a fait l'objet d'une des sanctions prévues au III de l'article L. 97-2 du CPCE ou à l'article L. 97-3 du CPCE.

Le II de l'article L. 97-2 du CPCE prévoit en outre un certain nombre d'obligations qui incombent au titulaire d'une autorisation d'exploitation d'une assignation déposée par la France auprès de l'UIT. À défaut de respect par ce dernier des obligations qui lui sont imposées par les textes législatifs et réglementaires, le III du même article prévoit que le ministre en charge des communications électroniques le met en demeure de s'y conformer. Si le titulaire ne donne pas suite à la mise en demeure, le ministre chargé des communications électroniques peut prononcer à son encontre l'une des sanctions prévues au 2° de l'article L. 36-11.

Enfin, conformément à l'article L. 97-3 du CPCE, est puni d'un emprisonnement de six mois et d'une amende de 75 000 euros le fait d'exploiter une assignation de fréquence relative à un système satellitaire déclarée par la France à l'UIT sans l'autorisation prévue à l'article L. 97-2, ou de poursuivre cette

exploitation en violation d'une décision de suspension ou de retrait ou d'un constat de caducité de cette autorisation.

2. Le dispositif proposé

Le **I du présent article** modifie substantiellement l'article L. 97-2 du CPCE pour étendre les marges de manœuvre de l'État avant, durant et après le processus d'autorisation d'exploitation d'une assignation déposée par la France auprès de l'UIT.

Tout d'abord, les **alinéas 3 à 8** ajoutent deux réserves supplémentaires possibles au I de l'article 97-2 du CPCE, susceptibles de ne pas entraîner 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 ;

– et 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.

En outre, au 2 du I de l'article L. 97-2 du CPCE (**alinéas 9 à 17**) :

– est ajoutée une nouvelle condition pour obtenir une autorisation d'exploitation d'une fréquence à un système satellitaire, 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 (**alinéa 11**) ;

– est précisé que l'attribution de cette autorisation ne doit pas s'opposer aux besoins de la défense nationale ni au respect par la France de ses engagements internationaux, que le demandeur puisse démontrer l'existence d'un intérêt économique à ce que l'autorisation lui soit délivrée et qu'il ne soit pas dans l'incapacité technique ou financière de faire face durablement aux obligations résultant de l'obtention de l'autorisation.

Par ailleurs, les **alinéas 18 à 29** complètent le III de l'article L. 97-2 du CPCE pour préciser les sanctions auxquelles s'expose le titulaire d'une autorisation prévue au I du même article, dans l'hypothèse où il ne respecterait pas les obligations qui lui sont imposées. Le ministre chargé des communications électroniques pourra ainsi le mettre en demeure de respecter ses obligations puis, s'il n'est pas donné suite à cette mise en demeure, prononcer à son encontre une des différentes sanctions énumérées au même article.

Enfin, les **alinéas 30 à 38** réécrivent le VI de l'article L. 97-2 du CPCE en ajoutant trois alinéas :

– 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 ;

– et les modalités des procédures de mise en demeure et de sanction prévues dans la nouvelle rédaction du III.

En conséquence, le **II du présent article** procède à une actualisation de référence à l'article L. 97-4 du CPCE.

Il est enfin prévu au **III du présent article** que l'article s'applique à compter de l'entrée en vigueur du décret prévu au VI de l'article L. 97-2 et au plus tard le 31 décembre 2025.

3. Les modifications apportées par le Sénat

Le Sénat a adopté un amendement rédactionnel en commission à l'initiative des rapporteurs qui, d'une part, complète l'alinéa 14 en insérant les mots « que l'autorisation présente un intérêt économique pour la France », et d'autre part, à l'alinéa 27, insère le mot « pécuniaires » après les mots « des sanctions ».

4. La position de la commission

La commission a adopté six amendements rédactionnels de la rapporteure Anne Le Hénanff.

*

* *

TITRE III
RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DU SECTEUR FINANCIER

CHAPITRE IER
Dispositions modifiant le code monétaire et financier

Article 43 A

(art. L. 141-10 et L. 612-24-1 [nouveaux] du code monétaire et financier)

Désignation de la Banque de France et de l'Autorité de contrôle prudentiel et de résolution comme autorités compétentes dans le cas où une entité financière est assujettie à plusieurs autorités de supervision

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel adopté par le Sénat prévoit de désigner une seule autorité compétente pour exercer les fonctions et les missions prévues à l'article 19 du règlement DORA (déclaration des incidents majeurs liés aux technologies de l'information et de la communication et notification volontaire des cybermenaces importantes) à l'égard de deux catégories d'entité financière :

– la Banque de France pour les dépositaires centraux ;

– l'Autorité de contrôle prudentiel et de résolution (ACPR) pour les personnes morales relevant de sa compétence au sein du secteur de la banque, des services de paiement et des services d'investissement, à l'exception des entreprises de marché, ainsi qu'au sein du secteur de l'assurance, à l'exception des véhicules de titrisation.

➢ **Dernières modifications législatives intervenues**

L'article 43 A crée deux nouveaux articles dans le code monétaire et financier au sein du chapitre dédié aux missions de la Banque de France, d'une part, et, d'autre part, au sein de celui consacré à l'ACPR.

➢ **Modifications apportées par la commission**

La commission spéciale a désigné l'ACPR comme autorité compétente chargée de recevoir les déclarations des incidents majeurs liés aux TIC et les notifications de cybermenaces importantes de la part des entités financières qui relèvent de sa compétence tout en prévoyant une communication additionnelle à l'attention de l'Agence nationale de sécurité des systèmes d'information (ANSSI).

1. L'état du droit

L'article 19 du règlement DORA [1] de l'Union européenne (UE) du 14 décembre 2022 [2] encadre la déclaration des incidents majeurs liés aux technologies de l'information et de la communication (TIC) et la notification volontaire des cybermenaces importantes par les entités financières.

Considérant comme essentiel que le régime de notification des incidents majeurs liés aux TIC soit harmonisé, l'UE impose à toutes les entités financières de les notifier à leurs autorités compétences au moyen d'un cadre rationalisé unique. Au sens du règlement DORA, un incident majeur se caractérise par une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'entité financière.

De même, afin d'être cohérent avec la directive NIS 2 du 14 décembre 2022 [3], l'UE autorise ces entités à notifier volontairement à ces mêmes autorités les cybermenaces importantes qu'elles estiment pertinentes pour le système financier, les utilisateurs de services ou les clients. Telle que définies par le règlement, celles-ci présentent des caractéristiques techniques indiquant qu'elles pourraient donner lieu à un incident majeur lié au TIC ou à un incident opérationnel ou de sécurité majeur lié au paiement.

L'article 19 du règlement DORA précise en outre que « *lorsqu'une entité financière est soumise à la surveillance de plusieurs autorités nationales compétentes* […]*, les États membres désignent une seule autorité compétente* ».

(1) Acronyme en anglais de Digital Operational Resilience Act.

(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° 600/2014, (UE) n° 909/2024 et (UE) 2016/1011.

(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.

Les entités financières

En application de l'article 2 du règlement DORA, les entités financières correspondent aux :

– établissements de crédit ;

– établissements de paiement ;

– prestataires de service d'information sur les comptes ;

– établissements de monnaie électronique ;

– entreprises d'investissement ;

– prestataires de services sur crypto-actifs ;

– dépositaires centraux de titres ;

– contreparties centrales ;

– plateformes de négociation ;

– référentiels centraux ;

– gestionnaires de fonds d'investissement alternatifs ;

– sociétés de gestion ;

– prestataires de services de communication de données ;

– entreprises d'assurance et de réassurance ;

– intermédiaires d'assurance, de réassurance et d'assurance à titre accessoire ;

– institutions de retraite professionnelles ;

– agences de notation de crédit ;

– administrations d'indices de référence d'importance critique ;

– prestataires de services de financement participatif ;

– référentiels de titrisation.

2. Le dispositif proposé par le Sénat

La commission spéciale du Sénat a adopté un amendement du rapporteur Michel Canévet visant à désigner une seule autorité compétente pour exercer les fonctions et les missions prévues à l'article 19 du règlement DORA à l'égard de deux catégories d'entité financière :

– la Banque de France pour les dépositaires centraux ;

– l'Autorité de contrôle prudentiel et de résolution (ACPR) pour les personnes morales du secteur de la banque, des services de paiement et des services d'investissement qui relèvent de sa compétence, à l'exception des entreprises de marché.

Pour le rapporteur, « *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* ».

Les dépositaires centraux sont responsables de l'enregistrement et de la conservation des titres financiers ainsi que de la livraison des titres contre paiement. En application de l'article L. 441-1 du code monétaire et financier, ces organismes sont supervisés par l'Autorité des marchés financiers (AMF) et par la Banque de France. Le dispositif proposé par le Sénat entend donc faire de cette dernière l'unique destinataire de leurs déclarations d'incidents majeurs liés aux TIC et de leurs notifications volontaires des cybermenaces importantes.

En ce qui concerne les entités financières placées sous la supervision de l'ACPR, la commission spéciale a voulu clarifier le rôle de cette autorité chargée de veiller à la préservation de la stabilité du système financier quant à la réception et au traitement des déclarations d'incidents majeurs et des notifications de cybermenaces.

L'idée des sénateurs est également d'éviter un risque de double assujettissement au règlement DORA et à la directive NIS 2. L'article 17 du projet de loi prévoit en effet que les entités essentielles et importantes « *notifient sans retard injustifié à l'autorité nationale de sécurité des systèmes d'information tout incident ayant un impact important sur la fourniture de leurs services* », conformément à l'article 23 de la directive.

En séance, le gouvernement s'est opposé au dispositif proposé par la commission spéciale. Il a présenté un amendement prévoyant que la Banque de France et l'ACPR « *veillent* [seulement] *au respect* » du règlement DORA au lieu d'exercer les fonctions et missions prévues à son article 19.

Il considère que l'articulation du règlement DORA et de la directive NIS 2 en ce qui concerne la déclaration des incidents majeurs liés aux TIC et la notification volontaire des cybermenaces par les entités financières est déjà satisfaite. D'après lui, cet article additionnel au projet de loi risque de priver certaines entités financières de l'appui de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en désignant l'ACPR comme unique destinataire des déclarations et notifications prévues à l'article 19 du règlement DORA.

En séance, les sénateurs ont suivi l'avis de la commission spéciale en adoptant un sous-amendement à l'amendement du gouvernement supprimant

l'essentiel de son dispositif mais conservant la correction d'une erreur de référence relative à la liste des entreprises devant adresser à l'ACPR leurs déclarations d'incidents majeurs liés au TIC et leurs notifications de cybermenaces importantes.

3. La position de la commission

Tant au cours des auditions de la commission spéciale que de celles conduites par le rapporteur thématique Mickaël Bouloux, il a été mis en avant à plusieurs reprises la nécessité d'inclure l'ANSSI dans les destinataires des déclarations d'incidents majeurs liés aux TIC et des notifications de cybermenaces importantes de la part des entités financières.

Si l'ACPR est compétente pour apprécier l'impact financier des incidents, elle ne dispose ni du mandat ni des moyens techniques pour accompagner les entités dans leur gestion opérationnelle, qui relève davantage de la compétence de l'ANSSI.

En l'état de la rédaction issue de l'examen du projet de loi par le Sénat, l'ACPR se verrait contrainte de transmettre les déclarations qu'elle reçoit à l'ANSSI, ce qui engendrerait des délais importants, notamment en cas d'incidents de nuit ou en fin de semaine, celle-ci ne disposant ni d'un système d'astreinte ni d'un portail de déclaration accessible en continu, contrairement à l'ANSSI.

Dans ce contexte, il est apparu à la commission spéciale qu'une information directe et simultanée des autorités financières demeurait indispensable pour permettre une réaction rapide, prévenir tout risque de contagion et sécuriser les intérêts des clients.

Après avoir examiné plusieurs amendements ayant également pour objet de faire de l'ANSSI le destinataire des déclarations et notifications évoquées mais selon des modalités différentes, la commission spéciale a adopté l'amendement de M. Paul Midy visant à :

– désigner l'ACPR comme autorité compétente chargée de recevoir les déclarations d'incidents majeurs liés aux TIC et les notifications volontaires de cybermenaces importantes des entités financières qui relèvent de sa compétence en application de l'article 19 du règlement DORA ;

– prévoir que l'ANSSI est également destinataire de ces déclarations et notifications lorsque l'entité financière est également soumise aux dispositions de la directive NIS 2 en tant qu'entité essentielle ou importante ;

– étendre l'application de ces dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna [(1)].

(1) Cf. commentaire de l'article 56.

*

* *

Article 43
(art. L. 314-1 du code monétaire et financier)
Modification de la définition des prestataires de services techniques

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article remplace le terme de « technologie de l'information » par « technologie de l'information et de la communication » (TIC) à l'article L. 314-1 du code monétaire et financier qui définit les services de paiement.

Il s'agit d'une transposition de l'article 7 de la directive DORA qui elle-même met en cohérence avec le règlement éponyme l'article 3 de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP 2) que l'article L. 314-1 transpose déjà en droit interne.

➢ **Dernières modifications législatives intervenues**

L'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive DSP 2 est à l'origine de la version actuellement en vigueur de la définition des services de paiement et plus particulièrement de l'exclusion de leur champ de la fourniture de service par un prestataire technique.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

L'article L. 314-1 du code monétaire et financier détermine ce qu'est un service de paiement. Il exclut notamment de son champ l'assistance d'un prestataire technique à l'appui de la fourniture de ces services de paiement ainsi que l'équipement et la maintenance des terminaux et dispositifs utilisés à ces fins.

Cette prestation technique consiste 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 et la fourniture des réseaux de communication.

L'exclusion de cette activité du champ des services de paiement est une transposition de l'article 3 de la seconde directive de l'Union européenne (UE) sur les services de paiement (DSP 2) du 25 novembre 2015 (1) par l'article 6 de l'ordonnance n° 2017-1252 du 9 août 2017 (2).

2. Le dispositif proposé

L'article 7 de la directive de l'UE sur la résilience opérationnelle numérique du secteur financier (DORA (3)) du 14 décembre 2022 (4) modifie l'article 3 de la directive DSP 2 pour faire mention des technologies de l'information « *et de la communication* » (TIC) dans la définition de la fourniture de services par un prestataire de services techniques à l'appui de la fourniture de services de paiement.

Il s'agit de la dénomination employée par le règlement DORA (5) dont le premier considérant rappelle qu'à l'ère numérique les TIC « *sous-tendent les systèmes complexes qui sont utilisés dans les activités quotidiennes,* [qu'elles] *contribuent à la bonne marche de nos économies dans des secteurs clés, tels que le secteur financier, et* [qu'elles] *améliorent le fonctionnement du marché intérieur* ».

Cette évolution nécessite donc la modification de l'article L. 314-1 du code monétaire et financier qui définit les services de paiement.

3. Les modifications apportées par le Sénat

Cet article a été adopté sans modification par le Sénat.

4. La position de la commission

La commission spéciale a adopté cet article sans modifications.

---

(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.

(2) Ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

(3) Acronyme en anglais de Digital Operational Resilience Act.

(4) 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.

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

*
* *

Article 44
(art. L. 420-3 du code monétaire et financier)
Maintien de la résilience opérationnelle des gestionnaires de plates-formes de négociation

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit de modifier le I et le III de l'article L. 420-3 du code monétaire et financier, qui détermine les exigences organisationnelles auxquelles doivent répondre les gestionnaires de plates-formes de négociation, afin de transposer l'article 6 § 4 de la directive DORA sur la résilience opérationnelle numérique du secteur financier, qui modifie elle-même la directive MIFID 2 sur les marchés financiers dont sont issues les dispositions de droit interne visées.

Le règlement DORA fixe un certain nombre d'exigences en ce qui concerne la gestion du risque lié aux technologies de l'information et de la communication ainsi que les tests de résilience opérationnelle numérique. L'article 44 du projet de loi prévoit donc qu'il soit expressément fait référence à ces règles européennes.

➢ **Dernières modifications législatives intervenues**

Les dispositions concernées de l'article L. 420-3 du code monétaire et financier ont été introduites par l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers qui transposait la directive MIFID 2.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les articles L. 420-3 à L. 420-8 du code monétaire et financier déterminent les exigences organisationnelles auxquelles doivent se soumettre les plates-formes de négociation.

En application de l'article L. 420-1, une plate-forme de négociation peut prendre trois formes différentes qui constituent toujours au moins « *un système multilatéral qui assure la rencontre en son sein* […] *de multiples intérêts acheteurs et vendeurs exprimés par des tiers* » :

– le marché réglementé d'instruments financiers (article L. 421-1) ;

– le système multilatéral de négociation (article L. 424-1) ;

– le système organisé de négociation (article L. 425-1).

FORMES PRISES PAR LES PLATEFORMES DE NÉGOCIATION

Catégorie de plate-forme de négociation	Règles de rencontre des intérêts acheteurs et vendeurs exprimés par des tiers	Objet de la négociation	Nombre de plates-formes agréées en France
Marché réglementé	Non discrétionnaires	Conclusion de contrats portant sur des instruments financiers admis à la négociation dans le cadre de règles et système du marché	3
Système multilatéral de négociation		Conclusion de transactions sur des instruments financiers	15
Système organisé de négociation	À la discrétion du gestionnaire	Conclusion de transactions sur des titres de créance, des produits financiers structurés, des quotas d'émission de gaz à effet de serre, des instruments dérivés et des produits énergétiques de gros	10

Source : commission spéciale.

Les trois marchés réglementés actuellement agréés par l'Autorité des marchés financiers (AMF) sont Euronext Paris SA (la Bourse de Paris), le marché à terme international de France (MATIF) et le marché des options négociables de Paris (MONEP).

Ces plates-formes doivent répondre à un certain nombre d'exigences, parmi lesquelles se trouve la mise en place de systèmes, de procédures et de mécanismes efficaces :

– assurant que leurs systèmes de négociation sont résilients, possèdent une capacité suffisante de gestion de volumes élevés d'ordres et de messages et permettent un processus de négociation ordonné en période de tension sur les marchés ;

– exigeant des personnes utilisant des systèmes de négociation algorithmique qu'elles procèdent à des tests appropriés d'algorithmes et disposent d'environnements de tests, afin de s'assurer que les systèmes de négociation algorithmique ne créent pas ou ne contribuent pas à des conditions de négociation de nature à perturber le bon ordre du marché.

Ces dispositions ont été introduites par l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers qui transposait la seconde directive de l'Union européenne (UE) sur les marchés d'instruments financiers (MIFID 2 [1]) en date du 15 mai 2014 [2].

2. Le dispositif proposé

L'article 6 (§ 4) de la directive sur la résilience opérationnelle numérique du secteur financier (DORA) du 14 décembre 2022 [3] modifie notamment l'article 48 (§ 1 et § 6) de la directive MIFID 2 en ce qui concerne la résilience opérationnelle des gestionnaires de plates-formes de négociation.

Celle-ci doit être désormais répondre aux exigences prévues aux chapitres II et IV du règlement DORA [4] respectivement relatifs à la gestion du risque lié aux technologies de l'information et de la communication (TIC) et aux tests de résilience opérationnelle numérique.

En conséquence, l'article 44 du projet de loi prévoit de modifier l'article L. 420-3 du code monétaire et financier de manière que ses dispositions mentionnent expressément le respect du règlement DORA. Il entend aussi préciser que la mise en place de mécanismes assurant la continuité des activités en cas de défaillance imprévue des systèmes de négociation doit s'exécuter conformément à l'article 11 du règlement DORA qui détaille les modalités de mise en œuvre d'une politique complète de continuité des activités de TIC par les entités financières.

À noter également que le projet de loi rapproche le droit interne du droit de l'UE en prévoyant que les systèmes de négociation des plates-formes doivent être soumis à des tests « *exhaustifs* » afin de confirmer que les conditions de résilience opérationnelle des gestionnaires soient réunies en toutes circonstances et plus seulement « *dans des situations d'extrême volatilité des marchés* ».

3. Les modifications apportées par le Sénat

Cet article a été adopté sans modification par le Sénat.

---

(1) Acronyme en anglais de Markets in Financial Instruments Directive.

(2) 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.

(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.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 45
(art. L. 421-4 et L. 421-11 du code monétaire et financier)
Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article introduit une référence au chapitre II du règlement DORA relatif à la gestion du risque lié aux technologies de l'information et de la communication dans les dispositions que sont tenues de prendre les sociétés qui gèrent un marché réglementé.

➢ **Dernières modifications législatives intervenues**

Les dispositions relatives aux obligations des entreprises de marché mentionnées par l'article 45 ont été introduites par l'ordonnance n° 2007-544 du 12 avril 2007 relative aux marchés d'instruments financiers qui transposait la directive MIFID 2.

➢ **Modifications apportées par le Sénat**

Cet article a été modifié par un amendement rédactionnel.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté cet article sans modifications.

1. L'état du droit

Un marché réglementé est une catégorie de plate-forme de négociation (1) qui constitue un système multilatéral assurant ou facilitant la rencontre, en son sein et selon des règles non discrétionnaires, de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des instruments financiers, d'une manière qui aboutisse à la conclusion de contrats portant sur les instruments financiers admis à la

(1) Cf. *commentaire de l'article 44.*

négociation dans le cadre des règles et systèmes de ce marché, ainsi que le définit l'article L. 421-1 du code monétaire et financier.

Il est géré par une entreprise de marché prenant la forme d'une société commerciale aux termes de l'article L. 421-2. Les trois marchés réglementés qui existent en France sont tous gérés par l'entreprise Euronext : le marché des actions (communément appelé « Bourse de Paris ») et les deux marchés de produits dérivés (le MATIF [1] et le MONEP [2]).

En application de l'article L. 421-11, cette entreprise de marché est tenue de prendre les dispositions nécessaires en vue notamment 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 réglementé qu'elle gère et prendre les mesures appropriées pour atténuer ces risques ;

– garantir le bon fonctionnement des systèmes techniques de négociation et disposer notamment de procédures d'urgence destinées à faire face aux éventuels dysfonctionnements.

Un arrêté du ministre chargé de l'économie, pris après l'avis de l'Autorité des marchés financiers (AMF) et du Comité consultatif de la législation et de la réglementation financières (CCLRF), détermine les règles relatives à ces deux obligations. Il revient également à l'AMF de s'assurer de la bonne application de ces règles, en s'appuyant notamment sur les contrôles effectués par l'Autorité de contrôle prudentiel et de résolution (ACPR), comme le prévoient les articles L. 421-4 et L. 421-11.

Ces dispositions sont conformes à l'article 47 de la seconde directive sur les marchés d'instruments financiers [3] (MIFID [4] 2). Elles avaient été introduites en droit interne par l'ordonnance n° 2007-544 du 12 avril 2007 relative aux marchés d'instruments financiers qui transposait la première directive MIFID [5].

2. Le dispositif proposé

L'article 45 du projet de loi introduit une référence aux exigences introduites par le chapitre II du règlement de l'UE du 14 décembre 2022 sur la

---

(1) Acronyme originel de marché à terme international de France.

(2) Marché des options négociables de Paris.

(3) 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.

(4) Markets in Financial Instruments Directive *(en anglais).*

(5) Directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers, modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil.

résilience opérationnelle numérique du secteur financier [1] (DORA [2]) dans les obligations auxquelles sont astreintes les entreprises de marché.

Le chapitre II du règlement DORA traite de la gestion du risque lié aux technologies de l'information et de la communication (TIC). L'article 6 de la directive éponyme [3] modifie en conséquence l'article 47 de la directive MIFID 2 afin que les États membres exigent des marchés réglementés « *qu'ils soient adéquatement équipés pour gérer les risques auxquels ils sont exposés, y compris le risque lié aux TIC conformément au chapitre II du règlement* [DORA]*, qu'ils mettent en œuvre des dispositifs et des systèmes appropriés leur permettant de cerner les risques significatifs pouvant compromettre leur bon fonctionnement, et qu'ils instaurent des mesures effectives pour atténuer ces risques* ».

L'article 45 du projet de loi propose donc de modifier l'article L. 421-11 du code monétaire et financier, ainsi que l'article L. 421-4 par coordination, afin d'y introduire cette référence au nouveau cadre européen de gestion des risques en matière de TIC.

3. Les modifications apportées par le Sénat

La commission spéciale a adopté un amendement rédactionnel du rapporteur Michel Canévet.

4. La position de la commission

La commission spéciale a adopté cet article sans le modifier.

---

(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) Digital Operational Resilience Act *(en anglais).*

(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.

*

* *

Article 45 bis

(art. L. 54-10-7 et L. 421-11-1 [nouveau] du code monétaire et financier)

Désignation de l'Autorité des marchés financiers comme autorité compétente dans le cas où une entreprise de marché ou un prestataire de services pour crypto-actifs est assujetti à plusieurs autorités de supervision

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel adopté par le Sénat prévoit de désigner l'Autorité des marchés financiers (AMF) comme seule autorité compétente pour exercer les fonctions et les missions prévues à l'article 19 du règlement DORA (déclaration des incidents majeurs liés aux technologies de l'information et de la communication et notification volontaire des cybermenaces importantes) à l'égard de deux catégories d'entité financière :

– les prestataires de services de crypto-actifs ;

– les entreprises de marché.

Cette proposition s'inscrit dans la continuité de l'article 43 A (nouveau) du projet de loi qui confère le même rôle à la Banque de France et à l'Autorité de contrôle prudentiel et de résolution (ACPR) à l'égard d'autres entités financières.

➢ **Dernières modifications législatives intervenues**

L'article 45 *bis* complète l'article L. 54-10-7 du code monétaire financier qui a été créé par l'article 18 de l'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés de crypto-actifs.

Il insère également un article L. 421-11-1 à ce même code au sein de la sous-section consacrée aux obligations des entreprises de marché.

➢ **Modifications apportées par la commission**

La commission spéciale a désigné l'AMF comme autorité compétente chargée de recevoir les déclarations des incidents majeurs liés aux TIC et les notifications de cybermenaces importantes de la part des entités financières qui relèvent de sa compétence tout en prévoyant une communication additionnelle à l'attention de l'Agence nationale de sécurité des systèmes d'information (ANSSI) par le biais d'un formulaire unique.

1. L'état du droit

L'article 19 du règlement DORA du 14 décembre 2022 (1) encadre la déclaration des incidents majeurs liés aux technologies de l'information et de la communication (TIC) et la notification volontaire des cybermenaces importantes par les entités financières (2).

Aux termes de cet acte, toutes les entités financières doivent notifier les incidents majeurs à leurs autorités compétentes au moyen d'un cadre rationalisé unique. De même, ces entités sont autorisées à notifier volontairement à ces mêmes autorités les cybermenaces importantes qu'elles estiment pertinentes pour le système financier, les utilisateurs de services ou les clients.

L'article 19 du règlement DORA précise en outre que « *lorsqu'une entité financière est soumise à la surveillance de plusieurs autorités nationales compétentes* […]*, les États membres désignent une seule autorité compétente* ».

2. Le dispositif proposé par le Sénat

Par analogie avec la désignation, à l'article 43 A (nouveau), de la Banque de France et de l'Autorité de contrôle prudentiel et de résolution (ACPR) comme autorités respectivement compétentes pour les dépositaires centraux et pour la plupart des personnes morales du secteur de la banque et de l'assurance, le Sénat a également désigné l'Autorité des marchés financiers (AMF) comme autorité compétente pour :

– les prestataires de services sur crypto-actifs ;

– les entreprises de marché.

Cet ajout résulte de l'adoption en séance, contre l'avis du gouvernement, d'un amendement du rapporteur Michel Canévet. D'après lui, « *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* ».

L'AMF se voit déjà soumettre les demandes d'agrément des prestataires de services sur crypto-actifs en application de l'article L. 54-10-7 du code monétaire et financier que le Sénat propose ainsi de compléter.

En ce qui concerne les entreprises de marché, en charge de la gestion des marchés réglementés (3), l'AMF vérifie la conformité des règles qu'elles édictent

---

(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° 600/2014, (UE) n° 909/2024 et (UE) 2016/1011.

(2) Cf. *commentaire de l'article 43 A.*

(3) Cf. *commentaire de l'article 45.*

aux lois et aux règlements (1) et s'assure de la bonne application des dispositions auxquelles elles sont astreintes (2). C'est également cette autorité qui propose au ministre chargé de l'économie la reconnaissance d'un marché réglementé (3).

Si le gouvernement avait également proposé que l'AMF soit destinataire des déclarations d'incidents majeurs liés aux TIC et de la notification volontaire des cybermenaces importantes pour les prestataires de services de crypto-actifs (4) et pour les entreprises de marché (5) , il souhaitait néanmoins prévoir que, pour ces dernières, elles transmettent également ces signalements à l'Agence nationale de sécurité des systèmes d'information (ANSSI), notamment lorsqu'elles sont aussi soumises, en tant qu'entités essentielles, au titre II du projet de loi transposant la directive dite NIS 2 (6).

Ce débat rejoint celui posé lors de la discussion de l'article 43 A concernant la désignation de la Banque de France et de l'ACPR comme autorités compétentes au titre de l'application de l'article 19 du règlement DORA et la question du double assujettissement à celui-ci et la directive NIS 2.

3. La position de la commission

À l'instar des entités financières relevant de l'ACPR (7), la commission spéciale a adopté trois amendements identiques (du président, du rapporteur général et du rapporteur thématique Mickaël Bouloux) visant à désigner l'AMF comme destinataire des déclarations d'incidents majeurs liés aux TIC et des notifications de cybermenaces importantes des entités financières qu'elle supervise, tout en prévoyant une communication additionnelle à l'ANSSI.

Toutefois, les amendements adoptés précisent que « *les déclarations et notifications mentionnées* […] *sont réalisées par le biais d'un document unique transmis simultanément* » à l'AMF et à l'ANSSI, ce qui n'est pas le cas à l'article 43 A modifié par la commission spéciale.

L'application de l'article 45 *bis* est également étendu à la Nouvelle-Calédonie, à la Polynésie française et aux îles Wallis et Futuna.

---

(1) Article L. 421-10.

(2) Article L. 421-11.

(3) Article L. 421-4.

(4) Amendement n° 111.

(5) Amendement n° 112.

(6) 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.

(7) Cf. commentaire de l'article 43 A.

*

* *

Article 46

(art. L. 511-41-1-B du code monétaire et financier)

Références aux risques liés aux technologies de l'information et de la communication au sein des dispositifs de gestion des risques des établissements de crédit et des sociétés de financement

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit de transposer l'article 4 de la directive DORA qui met en cohérence les exigences prudentielles auxquelles sont soumis les prestataires de services bancaires avec la prise en compte renforcée du risque lié aux technologies de l'information et de la communication par le règlement éponyme.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été créées par l'article 3 de l'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 qui transposait la directive CRD (*Capital Requirements Directive*) du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les prestataires de services bancaires sont tenus de prendre des dispositions prudentielles consistant à respecter des normes de gestion destinées à garantir leur liquidité et leur solvabilité à l'égard des déposants et des tiers, ainsi que l'équilibre de leur structure financière, en application de l'article L. 511-41 du code monétaire et financier.

Les prestataires de services bancaires

Les prestataires de services bancaires appartiennent à la catégorie des prestataires de services qui font l'objet du livre V de la partie législative du code monétaire et financier (1).

Ils sont constitués des établissements de crédit et des sociétés de financement.

Les premiers sont les entreprises dont l'activité consiste en une ou plusieurs activités suivantes (2) :

– recevoir du public des dépôts ou d'autres fonds remboursables et octroyer des crédits pour son propre compte ;

– exercer une activité de négociation pour compte propre ou une activité de prise ferme d'instruments financiers ou de placement d'instruments financiers avec engagement ferme, sous réserve de respecter des conditions tenant à la valeur totale des actifs de l'entreprise (au moins 30 milliards d'euros dans le cas général).

Il existe actuellement 877 établissements de crédit en France (3).

Les secondes sont des personnes morales, autres que des établissements de crédit, qui effectuent à titre de profession habituelle ou pour leur propre compte des opérations de crédit dans les conditions et limites définies par leur agrément (4). On compte aujourd'hui 144 sociétés de financement en France.

La principale différence entre une société de financement et un établissement de crédit est que la première ne peut effectuer que des opérations de crédit alors que le second délivre à la fois des crédits et reçoit des fonds remboursables du public, à l'instar des dépôts. À noter que le statut de société de financement est cumulable avec celui d'entreprise d'investissement, d'établissement de paiement ou d'établissement de monnaie électronique.

Parmi ces dispositions prudentielles figure, à l'article L. 511-41-1-B, l'obligation de mettre en place « *des dispositifs, stratégies et procédures faisant l'objet d'un contrôle interne régulier* […]*, leur permettant de détecter, de mesurer et de gérer les risques auxquels* [les prestataires de services bancaires] *sont ou pourraient être exposés du fait de leurs activités* ».

Les risques mentionnés sont :

---

(1) Cette catégorie comprend également les prestataires de services de paiement, les changeurs manuels, les émetteurs de monnaie électronique et de jetons de monnaie électronique, les prestataires de services d'investissements ainsi que divers prestataires de services comme les conseillers en investissements financiers, les sociétés de gestion de placements collectifs ou encore les prestataires et intermédiaires en financement participatif.

(2) Conformément à l'article 4 du 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 modifiant le règlement (UE) n° 648/2012, auquel fait référence l'article L. 511-1 du code monétaire et financier.

(3) Registre des agents financiers (REGAFI).

(4) Article L. 511-1.

– le risque de crédit et de contrepartie, y compris le risque résiduel ;

– le risque de concentration lié aux expositions sur des contreparties ;

– le risque généré par les opérations de titrisation ;

– les risques de marché ;

– les risques de variation des taux d'intérêt et de variation des écarts de crédit lorsque ces variations affectent la valeur économique des fonds propres et les produits d'intérêts nets de leurs activités hors portefeuille de négociation ;

– le risque opérationnel ;

– le risque de liquidité ;

– le risque de levier excessif ;

– les risques mis en évidence dans le cadre de tests de résistance régulièrement mis en œuvre.

En fonction de la nature des risques encourus, les prestataires de services bancaires sont tenus d'établir des plans d'urgence et de poursuite de leur activité, de maintenir des coussins adéquats de liquidité et de disposer de plans de rétablissement de leur liquidité.

Ces dispositions ont été introduites par l'article 3 de l'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. Elles transposent la directive CRD [(1)] du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle [(2)] qui, elle-même, met en cohérence le droit de l'UE avec les normes internationales établies par les seconds accords de Bâle.

2. Le dispositif proposé

L'article 4 de la directive Digital Operational Resilience Act (DORA) du 14 décembre 2022 [(3)] modifie notamment les articles 85 et 97 de la directive CRD

(1) Capital Requirements Directive *(en anglais).*

(2) 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.

(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.

afin de mettre en cohérence les exigences prudentielles avec le nouveau cadre posé par le règlement DORA du même jour [(1)].

Au quatrième considérant de la directive DORA, il est en effet rappelé que la directive CRD n'énonce que des règles générales de gouvernance interne.

Le risque lié aux technologies de l'information et de la communication n'y est traité que de manière implicite sur la base de la prévention du risque opérationnel à l'article 85 de la directive CRD. Ce risque désigne l'éventualité de pertes découlant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes internes ou d'événements extérieurs, y compris le risque juridique [(2)].

La directive DORA entend désormais traiter le risque lié aux TIC « *explicitement et clairement* », notamment en incluant les plans de réponse et de rétablissement dans les exigences en matière de plans d'urgence et de poursuite de l'activité.

Ainsi, les risques mis en évidence par les tests de résilience opérationnelle numérique prévus par le règlement DORA doivent figurer parmi les dangers auxquels les prestataires de services bancaires sont susceptibles d'être exposés et qui doivent faire l'objet d'un processus de contrôle et d'évaluation prudentiel harmonisé au niveau de l'UE (SREP [(3)]). La directive DORA modifie en ce sens l'article 97 de la directive CRD.

L'article 46 du projet de loi prévoit donc d'inclure expressément les risques liés aux TIC, tels que définis par le règlement DORA, y compris ceux liés aux services de TIC fournis par les prestataires tiers, dans le périmètre du risque opérationnel.

Il ajoute également une dixième catégorie de risque correspondant à ceux « *mis en évidence par des tests de résilience opérationnelle numérique conformément au chapitre IV du règlement* [DORA] », ce dernier énonçant les exigences applicables à la réalisation de ces tests.

Enfin, le dispositif proposé par le gouvernement prévoit d'imposer aux établissements de crédit et aux sociétés de financement l'établissement de « *politiques* » d'urgence et de poursuite de leur activité et non plus seulement des « *plans* ». Ces derniers seraient complétés de « *plans de réponse et de rétablissement des* [TIC] *qu'ils utilisent pour la communication d'informations* ».

---

(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 4 du 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) no 648/2012.

(3) Supervisory Review and Evaluation Process *(en anglais).*

À noter que la directive CRD modifiée par la directive DORA ne vise que les établissements de crédit et non les sociétés de financement. Le gouvernement a néanmoins fait le choix d'étendre à ces dernières la transposition dans la mesure où « *ces sociétés sont confrontées aux mêmes risques en matière de sécurité des systèmes d'information* » comme le souligne le Conseil d'État dans son avis sur le projet de loi. Cet objectif lui apparaît cohérent avec la réglementation prudentielle qui traite ces sociétés de la même manière que les établissements de crédit.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas apporté de modification à cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 47

(art. L. 511-55 du code monétaire et financier)

Référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article transpose l'article 4 de la directive DORA en modifiant l'article L. 511-55 du code monétaire et financier qui oblige les prestataires de services bancaires à se doter d'un dispositif de gouvernance solide de manière à inclure les réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code monétaire et financier par l'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. Elles visaient à assurer la transposition de l'article 74 de la directive 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], dite CRD (*Capital Requirements Directive*).

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

Les établissements de crédit et les sociétés de financement constituent les deux catégories de prestataires de services bancaires [2]. Ils sont soumis à plusieurs règles en ce qui concerne leur organisation et leur contrôle interne.

Ainsi, l'article L. 511-55 du code monétaire et financier dispose que ces prestataires de services bancaires doivent se doter d'un dispositif de gouvernance solide comprenant notamment :

– une organisation claire assurant un partage des responsabilités bien défini, transparent et cohérent ;

– des procédures efficaces de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés ;

– un dispositif adéquat de contrôle interne ;

– des procédures administratives et comptables saines ;

– des politiques et pratiques de rémunération permettant et favorisant une gestion saine et efficace des risques ;

– un plan préventif de rétablissement, s'ils sont soumis à cette obligation.

Ces dispositions ont été introduites dans le code monétaire et financier par l'article 3 de l'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 et constituent une transposition de l'article 74 de la directive CRD du 26 juin 2013 [3].

---

(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) Cf. *commentaire de l'article 46.*

(3) 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. Le dispositif proposé

L'article 4 de la directive DORA du 14 décembre 2022 (1) modifie l'article 74 de la directive CRD. Au quatrième considérant de la directive DORA, il est en effet constaté les limites de cette dernière dans la mesure où celle-ci n'énonçait que des règles générales de gouvernance interne dans le domaine des services bancaires (2).

Désormais, les établissements de crédit doivent disposer d'un dispositif solide de gouvernance d'entreprise, comprenant notamment « *des réseaux et des systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554* (3) [DORA] ».

En conséquence, l'article 47 du projet de loi modifie l'article L. 511-55 du code monétaire et financier de sorte à ce que les établissements de crédit et les sociétés de financement se dotent « *de réseaux et de systèmes d'information mis en place et gérés conformément au règlement* [DORA] ». L'inclusion des sociétés de financement, alors que la directive CRD ainsi modifiée, ne vise que les établissements de crédit, se justifie par la similitude des risques auxquels elles sont exposées. Même s'il observe une forme de « sur-transposition », le Conseil d'État partage l'analyse du gouvernement (4), d'autant plus que ces deux prestataires de services bancaires sont d'ores et déjà soumis aux mêmes règles d'ordre prudentiel.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté cet article sans le modifier.

---

(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) Cf. *commentaire de l'article 46.*

(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) n° 909/2014 et (UE) 2016/1011.

(4) Cf. *commentaire de l'article 46.*

*

* *

Article 48
(art. L. 521-9 du code monétaire et financier)
Obligations des prestataires de services de paiement en matière de gestion du risque lié aux technologies de l'information et de la communication

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit que les prestataires de service de paiement respectent le cadre de gestion du risque lié aux technologies de l'information et de la communication établi par le règlement DORA du 14 décembre 2022 dans le cadre des procédures qu'ils sont tenus de mettre en place pour atténuer et contrôler les risques opérationnels de sécurité (article L. 521-9 du code monétaire et financier).

➢ **Dernières modifications législatives intervenues**

L'article L. 521-9 a été introduit dans le code monétaire et financier par l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP 2).

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

Au sens de l'article L. 521-1 du code monétaire et financier, les prestataires de services de paiement correspondent aux :

– établissements de paiement ;

– établissements de monnaie électronique ;

– établissements de crédit ;

– prestataires de services d'information sur les comptes.

La Banque de France [1], le Trésor public et la Caisse des dépôts et consignations (CDC) peuvent également être considérés comme de tels prestataires lorsqu'ils fournissent des services de paiement.

En vue de gérer les risques opérationnels et de sécurité liés à ces services, les prestataires en question sont tenus de mettre en place des procédures prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés, conformément à l'article 95 de la directive DSP 2 transposé à l'article L. 521-9 du code monétaire et financier [2].

Un arrêté du ministre en charge de l'économie et des finances du 3 novembre 2014 [3] précise le contenu de ces procédures.

(1) De même que l'Institut d'émission des départements d'outre-mer (IEDOM) et l'Institut d'émission d'outre-mer (IEOM) qui lui sont rattachés.

(2) Ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

(3) Titre VI bis *de l'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 soumis au contrôle de l'Autorité de contrôle prudentiel et de résolution.*

Les services de paiement

En application de l'article L. 314-1 du code monétaire et financier, les services de paiement désignent :

– les services permettant le versement ou le retrait d'espèces sur un compte de paiement et les opérations de gestion d'un compte de paiement ;

– l'exécution des opérations de paiement associées à un compte de paiement ou à une ouverture de crédit (prélèvements, paiements par carte, virements) ;

– l'émission d'instruments de paiement ou l'acquisition d'opérations de paiement ;

– les services de transmission de fonds ;

– les services d'initiation de paiement ;

– les services d'information sur les comptes.

Cette définition est issue de la seconde directive sur les services de paiement (DSP 2) du 25 novembre 2015 (1) (annexe I).

2. Le dispositif proposé

L'article 95 de la directive DSP 2 a été modifié par l'article 7 (§ 4) de la directive DORA du 14 décembre 2022 (2). Ce dernier prévoit que le cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité soit établi « *sans préjudice de l'application du chapitre II du règlement* [DORA] (3) » par les prestataires de services de paiement.

Le chapitre en question fixe un cadre de gestion du risque lié aux technologies de l'information et de la communication (TIC) par les entités financières dans l'Union européenne. Par analogie avec les articles 44 (gestionnaires de plates-formes de négociation), 45 (entreprises de marché) et 52 (prestataires de services d'investissement) du projet de loi, l'article 48 prévoit qu'il soit fait référence à ces dispositions du règlement DORA pour les prestataires de services de paiement.

---

(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.

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

L'article L. 521-9 serait complété par un alinéa précisant que ces derniers « *respectent en outre les exigences du chapitre II du règlement* [DORA] ».

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté cet article sans modification.

*

* *

Article 49

(art. L. 521-10 du code monétaire et financier)

Modification de la liste des prestataires de services de paiement soumis à une obligation de notification des incidents opérationnels ou de sécurité majeur

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoyait initialement de réserver les obligations de déclaration des incidents majeurs actuellement en vigueur pour l'ensemble des prestataires de services de paiement (article L. 521-10 du code monétaire et financier) à la Banque de France, au Trésor public et à la Caisse des dépôts et consignations du fait de l'entrée en application directe du règlement DORA du 14 décembre 2022 pour ce qui concerne les entités financières.

➢ **Dernières modifications législatives intervenues**

Les dispositions de l'article L. 521-10 ont été introduites par l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP 2).

➢ **Modifications apportées par le Sénat**

Cet article a été réécrit par le Sénat dans un souci de simplification afin, d'une part, de faire de l'Autorité de contrôle prudentiel et de résolution (ACPR) l'unique destinataire des déclarations d'incidents qu'elle doit ensuite déclarer à la Banque de France et, d'autre part, de prévoir expressément que les obligations déclaratives auxquelles sont soumises les entités financières fournissant des services de

paiement relèvent du règlement DORA. Le cas de la Caisse des dépôts et consignations demeure à part en raison de l'adoption à venir d'un nouveau décret relatif au contrôle interne et externe de celle-ci.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

Lorsqu'ils sont confrontés à un incident majeur, les prestataires de services de paiement sont tenus d'en informer dans les meilleurs délais l'ACPR, la Banque de France ou encore ses utilisateurs selon les cas de figure en application de l'article L. 521-10 du code monétaire et financier.

Tels que définis à l'article L. 521-1, les prestataires de services de paiement sont les établissements de paiement, les établissements de monnaie électronique, les établissements de crédit et les prestataires de services d'information sur les comptes [(1)]. Dès lors qu'ils fournissent des services de paiement, la Banque de France [(2)] , le Trésor public et la Caisse des dépôts et consignations (CDC) sont aussi considérés comme de tels prestataires.

En présence d'un incident opérationnel majeur, les prestataires de services de paiement doivent informer sans retard injustifié l'ACPR. S'il s'agit d'un incident de sécurité majeur, c'est la Banque de France qui est destinataire de l'information. Dans ce cas, elle évalue la gravité de l'événement et prend au besoin des mesures appropriées. Elle peut également en informer l'ACPR.

Pour le règlement DORA du 14 décembre 2022 [(3)], un incident opérationnel ou de sécurité majeur lié au paiement désigne « *un événement ou une série d'événements liés entre eux que les* [prestataires] *n'ont pas prévu, lié ou non aux technologies de l'information et de la communication* [TIC]*, qui une incidence négative élevée sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données liées au paiement ou sur les services liés au paiement fournis par l'entité financière* » (article 3 § 9 et 11).

La Banque de France et l'ACPR doivent ensuite communiquer dans les meilleurs délais les détails importants de l'événement à l'Autorité bancaire européenne (ABE) et à la Banque centrale européenne (BCE), voire à d'autres autorités nationales concernées si elles l'estiment nécessaire.

---

(1) Cf. *commentaire de l'article 48.*

(2) Y compris l'Institut d'émission des départements d'outre-mer (IEDOM) et l'Institut d'émission d'outre-mer (IEOM).

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

L'article L. 521-10 dispose également que les utilisateurs de services de paiement doivent être informés sans retard injustifié d'un incident ayant ou susceptible d'avoir des répercussions sur leurs intérêts financiers ainsi que de toutes les mesures disponibles qu'ils peuvent prendre pour atténuer les effets dommageables de l'incident.

Ces dispositions ont été introduites par l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP 2) [(1)].

2. Le dispositif proposé

Le chapitre III du règlement DORA établit désormais des règles uniformes de gestion, de classification et de notification des incidents liés aux TIC pour les entités financières, notamment en ce qui concerne :

– la déclaration des incidents majeurs liés aux TIC et la notification volontaire des cybermenaces importantes (article 19) [(2)] ;

– le retour d'information en matière de surveillance (article 22) ;

– les incidents opérationnels ou de sécurité liés au paiement concernant les prestataires de services de paiement (article 23).

Ce dernier article dispose que les exigences du chapitre III du règlement s'appliquent également aux incidents opérationnels ou de sécurité, majeurs ou non, des prestataires de paiement au sens strict, c'est-à-dire « *des établissements de paiement, des prestataires de services d'information sur les comptes et des établissements de monnaie électronique* ». La mention expresse de ces seules entités financières conduit donc l'article 7 (§ 5) de la directive DORA [(3)] à modifier l'article 96 de la directive DSP 2 pour que ses règles de notification des incidents ne s'appliquent plus à ces prestataires de services de paiement nommément désignés et éviter ainsi un chevauchement des obligations de notification aux autorités compétentes.

La transposition en droit interne de cette nouvelle directive implique donc de limiter le champ de l'article L. 521-10 du code monétaire et financier à la Banque de France (Institut d'émission des départements d'outre-mer et Institut d'émission en d'outre-mer inclus), au Trésor public et à la CDC, les autres prestataires de

---

(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.

(2) Cf. *commentaires des articles 43 A et 45* bis *du projet de loi.*

(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.

services de paiement au sens strict étant désormais soumis à l'application directe du chapitre III du règlement DORA.

La version initiale de l'article 49 du projet de loi prévoyait donc de modifier cet article pour ne viser expressément que les institutions et services mentionnés au II de l'article L. 521-1.

3. Les modifications apportées par le Sénat

Le Sénat a intégralement réécrit, avec l'avis favorable du gouvernement, l'article 49 du projet de loi.

a. En commission spéciale

La commission spéciale a adopté un amendement du rapporteur Michel Canévet visant à répercuter une partie des dispositions du règlement DORA dans la rédaction de l'article L. 521-10 tout en élargissant à la CDC les règles de déclaration désormais prévues pour les prestataires de services de paiement au sens strict. Il fait également de l'ACPR la seule destinataire des notifications.

Dans le détail, le texte adopté par la commission spéciale prévoit ainsi que :

– les prestataires de services de paiement déclarent à l'ACPR tout incident opérationnel ou de sécurité majeur lié au paiement ;

– les prestataires de services de paiement au sens strict ainsi que la CDC réalisent cette déclaration conformément à l'article 23 du règlement DORA [(1)] et dans les conditions prévues à l'article 19 [(2)] ;

– l'ACPR prend, au besoin, des mesures appropriées, conformément aux dispositions de l'article 22 [(3)], à l'exception des mesures relatives à la Banque de France, à l'IEDOM, à l'IEOM et au Trésor public ;

– l'ACPR communique ces incidents et les mesures prises à la Banque de France en application de l'article L. 631-1 [(4)] ;

---

(1) L'article 23 précise que le chapitre III Gestion, classification et notification des incidents liés aux TIC *s'applique bien aux incidents opérationnels ou de sécurité liés au paiement.*

(2) L'article 19 fixe les règles de déclaration des incidents majeurs liés aux TIC et de notification volontaire des cybermenaces importantes.

(3) L'article 22 prévoit que l'autorité compétence accuse réception de la notification initiale et de chaque rapport relatifs à un incident majeur lié au TIC ou à une cybermenace importante et qu'elle peut fournir en temps voulu à l'entité financière un retour d'information pertinent et adapté ou une orientation de haut niveau. Elle peut aussi examiner les mesures correctives appliquées et les moyens de réduire les effets préjudiciables dans le secteur financier.

(4) L'article L. 631-1 régit la coopération et les échanges d'informations entre la Banque de France, l'IEDOM, l'IEOM, l'ACPR et l'Autorité des marchés financiers (AMF).

– la Banque de France évalue les incidents opérationnels ou de sécurité majeurs liés au paiement et prend, au besoin, des mesures appropriées en informant l'ACPR.

Dans un souci de simplification, les sénateurs ont voulu faire de l'ACPR un point d'entrée unique pour les prestataires de services de paiement au sens strict et la CDC en supprimant ainsi la distinction entre les incidents opérationnels et les incidents de sécurité. L'application à la CDC des règles de notification du règlement DORA se justifie par le cadre prudentiel de ce groupe public comparable à celui des établissements de crédit.

b. En séance

L'article 49 modifié par la commission spéciale n'a pas fait l'objet d'un amendement du gouvernement.

Le rapporteur Michel Canévet a présenté un amendement visant à en corriger la rédaction pour tenir compte de la modification à venir du décret n° 2020-94 du 5 février 2020 relatif au contrôle interne et externe de la Caisse des dépôts et consignations qui devrait précisément tirer les conséquences de l'application du règlement DORA. La rédaction proposée fait référence à ce décret en Conseil d'État sur les obligations déclaratives de la CDC.

L'article ainsi modifié a été adopté par le Sénat avec l'avis favorable du gouvernement.

COMPARAISON DES RÉDACTIONS PROPOSÉES POUR L'ARTICLE L. 521-10 DU CODE MONÉTAIRE ET FINANCIER

Rédaction de l'article L. 521-10	Catégorie d'incident de paiement	Prestataire de services de paiement	Autorité destinataire
Texte en vigueur	incident opérationnel majeur	établissements de paiement, établissements de monnaie électronique, établissements de crédit, prestataires de services d'information sur les comptes	ACPR
		Banque de France, IEDOM et IEOM	
		Trésor public	
		Caisse des dépôts et consignations	
	incident de sécurité majeur	établissements de paiement, établissements de monnaie électronique, établissements de crédit, prestataires de services d'information sur les comptes	Banque de France (avec information de l'ACPR si nécessaire)
		Banque de France, IEDOM et IEOM	
		Trésor public	
		Caisse des dépôts et consignations	
Proposition du gouvernement	incident opérationnel majeur	Banque de France, IEDOM et IEOM	ACPR
		Trésor public	
		Caisse des dépôts et consignations	
	incident de sécurité majeur	Banque de France, IEDOM et IEOM	Banque de France (avec information de l'ACPR si nécessaire)
		Trésor public	
		Caisse des dépôts et consignations	
Proposition du Sénat	tout incident majeur (opérationnel ou de sécurité)	établissements de paiement, établissements de monnaie électronique, établissements de crédit, prestataires de services d'information sur les comptes (1)	ACPR (avec communication à la Banque de France)
		Caisse des dépôts et consignations (2)	
		Banque de France, IEDOM et IEOM	
		Trésor public	

(1) En précisant que les règles de déclaration obéissent à celles du chapitre III du règlement DORA.

(2) En précisant que les règles de déclaration obéissent : à celles du chapitre III du règlement DORA (en commission spéciale) ; à celles du décret du 5 février 2020 (en séance).

4. La position de la commission

La commission spéciale a adopté cet article sans le modifier.

*

* *

Article 49 bis
(art. L. 532-50 du code monétaire et financier)
Extension de l'application du règlement DORA aux succursales d'entreprises d'investissement de pays tiers

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel adopté par le Sénat prévoit d'étendre l'application du règlement Digital Operational Resilience Act (DORA) du 14 décembre 2022 aux succursales d'entreprises d'investissement de pays tiers afin de ne pas créer une rupture de l'égalité avec les autres prestataires de services d'investissement en France. En effet, le règlement DORA ne vise que les entreprises d'investissement *stricto sensu*.

➢ **Dernières modifications législatives intervenues**

L'article L. 532-50 du code monétaire et financier que le Sénat propose de compléter soumet les succursales d'entreprises d'investissement de pays tiers aux exigences prudentielles du règlement et de la directive *Investment Firms Regulations and Directive* (IFR-IFD) du 27 novembre 2019. Ses dispositions ont été introduites par l'article 77 de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

L'article L. 531-4 du code monétaire et financier définit les entreprises d'investissement comme des personnes morales agréées pour fournir à titre de profession habituelle des services d'investissement. Avec les sociétés de gestion de portefeuille et les établissements de crédit qui ont reçu un agrément en ce sens, elles appartiennent à la catégorie des prestataires de services d'investissement, conformément à l'article L. 531-1.

Les services d'investissement

En application de l'article L. 321-1 du code monétaire et financier, les services d'investissement portent sur les titres financiers (actions, titres de créance, parts d'organismes de placement collectif), les contrats financiers (instruments à terme) et les quotas d'émission de gaz à effet de serre.

Ils comprennent les services et activités suivants :

– la réception et la transmission d'ordres pour le compte de tiers ;

– 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 ;

– l'exploitation d'un système multilatéral de négociation ;

– l'exploitation d'un système organisé de négociation.

Cette liste est conforme à la directive du 15 mai 2014 concernant les marchés d'instruments financiers [(1)], dite MIFID 2 (*markets in financial instruments directive II*).

Une entreprise d'investissement doit satisfaire plusieurs conditions d'exercice, notamment en ce qui concerne les règles spécifiques relatives à une entreprise de pays tiers, c'est-à-dire « *une entreprise qui, si son administration centrale ou son siège social étaient situés dans un État membre de l'Union européenne* [UE]*, serait* […] *une entreprise d'investissement* » (article L. 532-47).

Celle-ci peut établir une succursale dans un État membre l'UE pour pouvoir fournir des services d'investissement à des clients, dès lors qu'elle a obtenu un agrément de l'autorité nationale compétente, soit l'Autorité de contrôle prudentiel et de résolution (ACPR) en la France.

À ce titre, l'article L. 532-50 prévoit que les dispositions du règlement du 27 novembre 2019 concernant les exigences prudentielles applicables aux

(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.

entreprises d'investissement [1] doivent être respectées par ces succursales d'entreprises de pays tiers, de même que plusieurs normes de gestion en droit interne transposées à partir de la directive du 27 novembre 2019 concernant la surveillance prudentielle de ces mêmes entreprises [2]. Ces deux actes législatifs de l'UE sont communément désignés ensemble sous l'acronyme IFR-IFD (*Investment Firms Regulations* et *Investment Firms Directive* en anglais).

2. Le dispositif proposé par le Sénat

La commission spéciale a adopté un amendement du rapporteur Michel Canévet portant article additionnel après l'article 49 du projet de loi.

Ces nouvelles dispositions étendent aux succursales d'entreprises d'investissement de pays tiers l'application du règlement DORA du 14 décembre 2022 [3], l'auteur de l'amendement soulignant que l'effet direct de cet acte législatif en droit interne ne permet pas d'inclure ces établissements. L'article 2 du règlement DORA ne mentionne que les entreprises d'investissement parmi les entités financières auxquelles ses dispositions s'appliquent.

Le rapporteur a considéré que « *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* ». Il a également défendu une analogie avec les exigences prudentielles qui s'imposent tant aux entreprises d'investissement de l'UE qu'aux succursales d'entreprises de pays tiers.

En séance, l'article additionnel a été adopté sans faire l'objet d'amendement du gouvernement.

3. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

---

(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) Directive (UE) 2019/2034 du Parlement européen et du Conseil du 27 novembre 2019 concernant la surveillance prudentielle des entreprises d'investissement et modifiant les directives 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE et 2014/65/UE.

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

*

* *

Article 50
(art. L. 533-2 du code monétaire et financier)
Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article transpose l'article 4 de la directive DORA en modifiant l'article L. 533-2 du code monétaire et financier, qui oblige les entreprises d'investissement et les entreprises de crédit qui fournissent des services d'investissement à se doter de dispositifs efficaces de contrôle et de sauvegarde de leurs systèmes informatiques, afin de faire référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites par l'ordonnance n° 2007-544 du 12 avril 2007 relative aux marchés d'instruments financiers. Elles sont conformes à l'article 74 de la directive CRD du 26 juin 2013.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

Les prestataires de services d'investissement (entreprises d'investissement, sociétés de gestion de portefeuille, établissements de crédit agréés [(1)]) doivent respecter plusieurs normes de gestion.

Parmi elles se trouve l'obligation pour les entreprises d'investissement et les établissements de crédit agréés de disposer de :

(1) Cf. *commentaire de l'article 49* bis.

– procédures administratives saines ;

– mécanismes de contrôle interne ;

– techniques efficaces d'évaluation des risques ;

– dispositifs efficaces de contrôle et de sauvegarde de leurs systèmes informatiques ;

– de techniques d'atténuation des risques pour les contrats dérivés de gré à gré non compensés par une contrepartie centrale.

Les sociétés de gestion de portefeuille ne sont pas concernées par ces obligations.

Ces dispositions figurant à l'article L. 533-2 du code monétaire et financier ont été, pour la plupart, introduites par l'article 4 de l'ordonnance n° 2007-544 du 12 avril 2007 relative aux marchés d'instruments financiers ainsi que par l'article 46 de la loi n° 2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires pour ce qui concerne les techniques d'atténuation des risques pour certains contrats dérivés.

La rédaction actuelle respecte l'article 74 de la directive 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)], dite « CRD » (Capital Requirements Directive).

2. Le dispositif proposé

L'article 4 de la directive Digital Operational Resilience Act (DORA) du 14 décembre 2022 [(2)] modifie l'article 74 de la directive CRD. Désormais, les entreprises d'investissement et l'ensemble des établissements de crédit, y compris donc ceux qui ont reçu un agrément pour fournir des services d'investissement conformément à l'article L. 531-1 du code précité, doivent disposer d'un dispositif solide de gouvernance d'entreprise, comprenant notamment « *des réseaux et des systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) 2022/2554* [(3)] [DORA] ».

Par analogie avec l'article 47 du projet de loi qui intégrait cette référence à l'article L. 511-55 au sujet de la gouvernance des établissements de crédit et des

---

(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) 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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

sociétés de financement [1], il est proposé que l'obligation faite aux prestataires de service d'investissement – autres que les sociétés de gestion de portefeuille – de se doter de « *dispositifs efficaces de contrôle et de sauvegarde de leurs systèmes informatiques* » concerne bien les « *réseaux et systèmes d'information mis en place et gérés conformément au règlement* [DORA] ».

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté cet article sans le modifier.

*

* *

Article 51
(art. L. 533-10 du code monétaire et financier)
Systèmes de technologies de l'information et de la communication et dispositifs de contrôle des prestataires de services d'investissement

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article transpose les articles premier et 6 de la directive DORA qui, elle-même, modifie deux directives sectorielles consacrées aux organismes de placement collectif en valeurs mobilières (OPCVM) et aux marchés d'instruments financiers (MIFID 2).

Il est question de faire référence au règlement DORA pour ce qui concerne plusieurs règles d'organisation auxquelles sont soumises les prestataires de services d'investissement en ce qui concerne les réseaux, les systèmes et les technologies de l'information et de la communication.

➢ **Dernières modifications législatives intervenues**

Les dispositions de l'article L. 533-10 ont été introduites dans le code monétaire et financier par l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers.

---

(1) Cf. *commentaire de l'article 47.*

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les différents prestataires de services d'investissement (entreprises d'investissement, sociétés de gestion de portefeuille et établissements de crédits agréés [(1)]) doivent obéir à plusieurs règles d'organisation.

L'article L. 533-10 du code monétaire et financier dispose que les sociétés de gestion de portefeuille ont l'obligation de :

– mettre en place des règles et procédures permettant de garantir le respect des dispositions qui leur sont applicables, y compris par les personnes placées sous leur autorité ou agissant pour leur compte (en particulier les conditions et limites dans lesquelles ces dernières peuvent effectuer pour leur propre compte des transactions personnelles) ;

– prendre toutes les mesures raisonnables pour empêcher les conflits d'intérêts de porter atteinte aux intérêts de leurs clients ;

– prendre des mesures raisonnables en utilisant des ressources et des procédures appropriées et proportionnées 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 ;

– conserver un enregistrement de tout service qu'elles fournissent et de toute transaction qu'elles effectuent, permettant à l'Autorité des marchés financiers (AMF) de contrôler le respect de leurs obligations et, en particulier, de toutes leurs obligations à l'égard des clients, notamment des clients potentiels.

(1) Cf. *commentaires de l'article 49* bis *et de l'article 50.*

Les sociétés de gestion de portefeuille

En application de l'article L. 532-9 du code monétaire et financier, les sociétés de gestion de portefeuille sont des personnes morales qui gèrent un ou plusieurs :

– organisme de placement collectif en valeurs mobilières (OPCVM) ;

– fonds d'investissement alternatif (FIA) ;

– autres placements collectifs.

Conformément à la définition de la directive du 13 juillet 2009 (1), un OPCVM est un organisme dont l'objet exclusif est le placement collectif en valeurs mobilières ou dans d'autres actifs financiers liquides des capitaux recueillis auprès du public et dont le fonctionnement est soumis au principe de la répartition des risques et dont les parts sont, à la demande des porteurs, rachetées ou remboursées, directement ou indirectement, à charge des actifs de ces organismes.

Quant aux FIA, ils correspondent à des organismes de placement collectif autres que les OPCVM qui lèvent des capitaux auprès d'un certain nombre d'investisseurs en vue de les investir, conformément à une politique d'investissement définie, dans l'intérêt de ces investisseurs, comme les entend la directive du 8 juin 2011 sur les gestionnaires de FIA (2).

Ces sociétés de gestion de portefeuille sont agréées par l'AMF.

Les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille, c'est-à-dire les entreprises d'investissement et les établissements de crédits à ce titre agréés, se soumettent à des conditions analogues.

Toutefois, l'article L. 533-10 précité précise, au 4° du II, que ces derniers doivent prendre des mesures raisonnables, en utilisant « *des systèmes* » – en plus des ressources et des procédures appropriées et proportionnées – pour garantir la continuité, la régularité mais aussi « *le caractère satisfaisant* » de la fourniture des services d'investissement, notamment lorsqu'ils confient à des tiers des fonctions « *ou d'autres tâches* » opérationnelles essentielles ou importantes. Il est en outre précisé que ces prestataires doivent éviter une aggravation indue du risque opérationnel.

La loi prévoit également que les entreprises d'investissement et les établissements de crédits agréés disposent en plus de 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

(1) 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.

(2) Directive 2011/61/UE du Parlement européen et du Conseil du 8 juin 2011 sur les gestionnaires de fonds d'investissement alternatifs et modifiant les directives 2003/41/CE et 2009/65/CE ainsi que les règlements (CE) n° 1060/2009 et (UE) n° 1095/2010.

autorisé et empêcher les fuites d'informations afin de maintenir en permanence la confidentialité des données (5° du II).

Ces dispositions ont été introduites par l'article 11 de l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers. Elles constituent une transposition de deux directives :

– la directive du 13 juillet 2009 concernant certains OPCVM, notamment son article 12 ;

– la directive du 15 mai 2014 concernant les marchés d'instruments financiers, dite MIFID 2 (*Markets in Financial Instruments Directive II*) (1), notamment son article 16.

2. Le dispositif proposé

La directive DORA du 14 décembre 2022 (2) modifie plusieurs directives sectorielles, dont les articles précités des directives OPCVM et MIFID 2.

L'article premier (§ 1) de la directive DORA amende l'article 12 de la directive OPCVM afin que les autorités compétentes de l'État membre d'origine d'une société de gestion de portefeuille exigent de celle-ci qu'elle ait « *des procédures administratives et comptables saines, 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] » (3).

En conséquence, le **1**° de l'article 51 du projet de loi propose de compléter le I de l'article L. 533-10 du code monétaire et financier par un 6° visant à ce que les sociétés de gestion de portefeuille, à l'exception de celles qui gèrent des FIA, mettent en place de telles procédures faisant référence aux « *réseaux et systèmes d'information mis en place et gérés conformément au règlement* [DORA] ». Cette mention est analogue à celles que le projet de loi envisage d'introduire :

– à l'article L. 511-55 par l'article 47 concernant les établissements de crédit et les sociétés de financement ;

– à l'article L. 533-2 par l'article 50 au sujet des entreprises d'investissement et des établissements de crédit fournissant des services d'investissement.

---

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

L'article 6 (§ 1) de la directive DORA modifie également l'article 16 de la directive MIFID 2 afin de prévoir que « *toute entreprise d'investissement prend des mesures raisonnables pour garantir la continuité et la régularité de la fourniture de ses services d'investissement et de l'exercice de ses activités d'investissement* » et qu'à cette fin « *elle utilise des systèmes appropriés et proportionnés, y compris des systèmes de technologies de l'information et de la communication* [TIC] *mis en place et gérés conformément à l'article 7 du règlement* [DORA] *ainsi que des ressources et des procédures appropriées et proportionnées* ».

Il précise également que les entreprises d'investissement assurent la sécurité et l'authentification des moyens de transfert de l'information conformément à ce même règlement.

Dès lors, le **2°** de l'article 51 du projet de loi vise à ce que les prestataires de services d'investissement – autres que les sociétés de gestion de portefeuille – utilisent des systèmes « *appropriés et proportionnés* », y compris des systèmes de TIC conformes au règlement précité, pour garantir la continuité des services d'investissement qu'ils offrent.

Il ajoute que la garantie de la sécurité et de l'authentification des moyens de transfert de l'information se fait aussi conformément au règlement DORA et procède, par la même occasion, à une correction rédactionnelle.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement du rapporteur thématique Mickaël Bouloux.

*

* *

Article 52

(art. L. 533-10-4 du code monétaire et financier)

Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article modifie l'article L. 533-10-4 du code monétaire et financier relatif à la prévention et à la résolution des incidents susceptibles d'affecter les activités de négociation algorithmique des entreprises d'investissement et des établissements de crédit agréés afin de transposer l'article 6 de la directive DORA du 14 décembre 2022 modifiant l'article 17 de la directive MIFID 2 du 15 mai 2014.

Celui-ci fait désormais référence aux exigences fixées par le règlement DORA en matière de gestion des risques liés aux technologies de l'information et de la communication, de réponse aux incidents, de rétablissement des services et de conduite de tests de résilience opérationnelle numérique.

➢ **Dernières modifications législatives intervenues**

Les dispositions de l'article L. 533-10-4 ont été introduites dans le code monétaire et financier par l'article 11 de l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers, transposant l'article 17 de la directive MIFID 2.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les prestataires de services d'investissement (entreprises d'investissement, sociétés de gestion de portefeuille, établissements de crédit agréés [1]) sont soumis à

(1) Cf. *commentaires des articles 49* bis*, 50 et 51.*

plusieurs règles d'organisation. Plusieurs d'entre elles régissent plus spécifiquement les activités de négociation algorithmique.

Celle-ci désigne la négociation d'instruments financiers dans laquelle un algorithme informatique détermine automatiquement les paramètres des ordres tels que l'opportunité ou le moment de leur émission, les conditions de prix ou de quantité ou la façon dont ils seront gérés après leur émission, sans intervention humaine ou avec une intervention humaine limitée. Cette définition, inscrite à l'article L. 533-10-3 du code monétaire et financier, est issue de la directive du 15 mai 2014 concernant les marchés d'instruments financiers [(1)] (MIFID 2 [(2)]).

En pratique, la négociation algorithmique prend, par exemple, la forme des paramètres d'ordre pour l'achat ou la vente d'actions (prix de saisie, volume de position, instant d'ouverture et de clôture…).

L'article L. 533-10-4 dispose que les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille, c'est-à-dire les entreprises d'investissement et les établissements de crédit agréés, ayant recours à la négociation algorithmique sont tenus de disposer de systèmes et contrôles des risques efficaces et adaptés à leur activité pour garantir que leurs systèmes de négociation :

– soient résilients et aient une capacité suffisante ;

– soient soumis à des seuils et limites de négociation appropriés ;

– préviennent l'envoi d'ordres erronés ou tout autre fonctionnement des systèmes susceptible de donner naissance ou de contribuer à une perturbation de marché ;

– ne puissent être utilisés à aucune fin contraire au règlement du 16 avril 2014 sur les abus de marché [(3)] ou aux règles d'une plate-forme de négociation à laquelle ces prestataires sont connectés.

Les entreprises d'investissement et les établissements de crédit agréés doivent, en outre, disposer de plans de continuité des activités efficaces pour faire face à toute défaillance de leurs systèmes de négociation et veiller à ce que ces derniers soient entièrement testés et convenablement suivis de manière à garantir leur conformité à ces exigences.

---

(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) Markets in Financial Instruments Directive II.

(3) Règlement (UE) n ° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission.

Ces dispositions ont été introduites dans le code monétaire et financier par l'article 11 de l'ordonnance n° 2016-827 du 23 juin 2016 relative aux marchés d'instruments financiers, transposant l'article 17 de la directive MIFID 2 précitée.

2. Le dispositif proposé

L'article 6 (§ 2) de la directive DORA du 14 décembre 2022 (1) modifie l'article 17 de la directive MIFID 2 pour mettre en cohérence ses dispositions avec le règlement DORA du même jour (2).

Tout d'abord, il prévoit que les systèmes et contrôles des risques dont disposent les entreprises d'investissement soient conformes aux exigences du chapitre II du règlement DORA, dédié à la gestion du risque lié aux technologies de l'information et de la communication (TIC). Cette référence est analogue à celles proposées aux articles 44 (gestionnaires de plate-forme de négociation), 45 (entreprises de marché) et 48 (prestataires de services de paiement) du projet de loi.

Concernant les mécanismes de continuité des activités, l'article 6 de la directive DORA amende également l'article 17 de la directive MIFID 2 de manière à ce qu'ils comprennent aussi « *une politique et des plans en matière de continuité des activités de TIC et de plans de réponse et de rétablissement des TIC mis en place conformément à l'article 11 du règlement* [DORA] ». Cet article détaille les modalités de réponse aux incidents et de rétablissement des services.

En outre, les systèmes de négociation de ces prestataires de services d'investissement doivent satisfaire les exigences spécifiques fixées aux chapitres II et IV du règlement DORA, ce dernier chapitre portant sur les tests de résilience opérationnelle numérique.

En conséquence, le présent article du projet de loi entend modifier l'article L. 533-10-4 du code monétaire et financier pour :

– préciser que l'obligation de résilience et de capacité suffisante des systèmes et contrôles des risques se fait conformément aux exigences du chapitre II du règlement DORA ;

– imposer que les prestataires disposent de « *mécanismes* » et non de « *plans* » de continuité des activités « *y compris d'une politique et de plans en matière de continuité des activités liées aux* [TIC] *et de plans de réponse et de rétablissement des* [TIC] *mis en place conformément à l'article 11 du règlement* [DORA] » ;

---

(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.

– faire en sorte que ces mécanismes soient testés et suivis de manière à garantir leur conformité aux chapitres II et IV du règlement DORA.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 53 (suppression maintenue)
(art. L. 612-24 du code monétaire et financier)
Référence aux prestataires informatiques critiques au sein des tiers auxquels l'Autorité de contrôle prudentiel et de résolution peut demander toute information

Suppression maintenue par la Commission

➢ **Résumé du dispositif et effets principaux**

Cet article incluait les prestataires tiers de services fondés sur les technologies de l'information et de la communication dans la liste des organismes susceptibles de devoir communiquer tous documents et renseignements à l'Autorité de contrôle prudentiel et de résolution (ACPR) à la demande de son secrétaire général en application de l'article L. 612-24 du code monétaire et financier.

La rédaction proposée était une transposition de l'article 4 de la directive DORA amendant l'article 65 de la directive CRD.

➢ **Dernières modifications législatives intervenues**

Ces dispositions avaient été introduites dans le code monétaire et financier par l'article 4 de l'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 qui transposait l'article 65 de la directive CRD.

➢ **Modifications apportées par le Sénat**

Cet article a été supprimé par le Sénat au motif que la rédaction actuelle de l'article L. 612-24 inclut déjà l'ensemble des tiers auprès desquels les personnes assujetties à l'ACPR ont externalisé des fonctions ou activités opérationnelles.

➢ **Modifications apportées par la commission**

La commission spéciale a maintenu la suppression de cet article.

1. L'état du droit

L'ACPR est chargée de veiller à la préservation de la stabilité du système financier et à la protection des clients, des assurées, des adhérents et des autres bénéficiaires des personnes qui sont soumises à son contrôle en application de l'article L. 612-1 du code monétaire et financier.

Ces personnes appartiennent au secteur de la banque, des services de paiement et des services d'investissement ainsi qu'à celui de l'assurance.

Pour exercer son contrôle, l'article L. 612-24 prévoit notamment que l'ACPR détermine la liste, le modèle, la fréquence et les délais de transmission des documents et des informations qui doivent lui être remis périodiquement.

À ce titre, son secrétaire général est habilité à demander tous renseignements et documents aux tiers auprès desquels les entités assujetties à son contrôle ont externalisé des fonctions ou activités opérationnelles. Il peut s'agir de rapports d'audit interne ou de contrats souscrits par exemple.

Ces dernières dispositions ont été introduites dans le code monétaire et financier par l'article 4 de l'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. Elles constituent une transposition de l'article 65 de la directive 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)], dite *Capital Requirements Directive* (CRD). Cette dernière met elle-même en œuvre les stipulations des seconds accords de Bâle de 2004.

2. Le dispositif proposé

L'article 4 de la directive DORA du 14 décembre 2022 [(2)] modifie l'article 65 de la directive CRD de manière à préciser que les tiers susceptibles de devoir communiquer leurs documents à leur autorité de supervision comprennent

---

(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) 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.

aussi les prestataires tiers de services de technologie de l'information et de la communication (TIC) visés au chapitre V du règlement DORA [1].

(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.

Le chapitre V du règlement DORA

Le cinquième chapitre du règlement DORA traite de la gestion des risques liés aux prestataires de services TIC.

Il détermine les principes clés pour une bonne gestion de ces dangers :

– principes généraux ;

– évaluation préliminaire du risque de concentration de TIC au niveau de l'entité financière ;

– principales dispositions contractuelles.

Le chapitre V établit également un cadre de supervision des prestataires tiers critiques de services TIC au travers de :

– la désignation de prestataires tiers critiques ;

– la structure du cadre de supervision ;

– les tâches du superviseur principal ;

– la coordination opérationnelle entre superviseurs principaux ;

– les pouvoirs du superviseur principal ;

– l'exercice des pouvoirs du superviseur principal en dehors de l'UE ;

– la demande d'informations ;

– les enquêtes générales ;

– les inspections ;

– la supervision continue ;

– l'harmonisation des conditions permettant l'exercice des activités de supervision ;

– le suivi par les autorités compétentes ;

– les redevances de supervision ;

– la coopération internationale.

En conséquence, l'article 53 du projet de loi proposait d'inscrire cette précision au troisième alinéa de l'article L. 612-24 du code monétaire et financier.

3. Les modifications apportées par le Sénat

La commission spéciale du Sénat a adopté un amendement du rapporteur Michel Canévet visant à supprimer cet article.

D'après lui, le secrétaire général de l'ACPR dispose déjà d'un pouvoir de communication des renseignements et documents nécessaires à l'accomplissement de sa mission de contrôle des entités financières de la part des prestataires tiers.

En effet, le troisième alinéa de l'article L. 612-24 prévoit que ce pouvoir s'exerce à l'égard des filiales des personnes assujetties « *ainsi qu'aux tiers auprès desquels ces personnes ont externalisé des fonctions ou activités opérationnelles* ».

Le rapporteur a observé que « *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* ».

En séance, aucun amendement visant au rétablissement de cet article n'a été déposé.

4. La position de la commission

La commission spéciale n'a pas rétabli cet article.

*

* *

Article 54

(art. L. 613-38 du code monétaire et financier)

Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit de modifier l'article L. 613-38 du code monétaire et financier de façon à ce que deux éléments compris dans les plans de résolution établis par le collège éponyme de l'Autorité de contrôle prudentiel et de résolution (ACPR) fassent référence à la résilience opérationnelle et numérique ainsi qu'aux réseaux et aux systèmes d'information mise en place et gérés conformément au règlement DORA du 14 décembre 2022.

L'article transpose ainsi l'article 5 de la directive éponyme qui elle-même modifie l'article 10 de la directive du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement (BRRD).

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code monétaire et financier par l'article 3 de l'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 qui transposait l'article 10 de la directive BRRD.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

L'ACPR comprend un collège de supervision, un collège de résolution et une commission des sanctions en application de l'article L. 612-4 du code monétaire et financier. Le second collège est notamment chargé d'établir des plans préventifs de résolution.

L'établissement de plans préventifs de résolution par ce collège fait partie des mesures de prévention et de gestion des crises bancaires, au même titre que :

– les plans préventifs de rétablissement ;

– l'analyse de résolvabilité ;

– l'exigence minimale de fonds propres et d'engagements éligibles ;

– les mesures d'intervention précoce ;

– les accords de soutien financier de groupe ;

– la valorisation ;

– les mesures de réduction et de conversion d'instruments de fonds propres ;

– la procédure de résolution.

Le collège de résolution de l'ACPR

Créé par la loi n° 2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires, le collège de résolution est présidé par le gouverneur de la Banque de France. Il est composé de six autres membres en application de l'article L. 612-8-1 :

– le directeur général du Trésor ;

– le président de l'Autorité des marchés financiers (AMF) ;

– un sous-gouverneur de la Banque de France ;

– le président de la chambre commerciale, financière et économique de la Cour de cassation ;

– le président du directoire du fonds de garantie des dépôts et de résolution (FGDR) ;

– le vice-président du collège de supervision de l'ACPR.

Cette instance exerce ses pouvoirs en matière de résolution des crises bancaires en ce qui concerne les établissements de crédit, les compagnies financières holding, les compagnies financières holding mixtes, les établissements financiers et les entreprises d'investissements, conformément à l'article L. 612-1.

Elle constitue l'autorité de résolution nationale pour la France au sens du règlement (UE) n° 806/2014 du Parlement européen et du Conseil du 15 juillet 2014 établissant des règles et une procédure uniformes pour la résolution des établissements de crédit et de certaines entreprises d'investissement dans le cadre d'un mécanisme de résolution unique et d'un fonds de résolution bancaire unique, et modifiant le règlement (UE) n° 1093/2010.

L'article L. 613-38 dispose notamment que les plans préventifs de résolution comprennent un certain nombre d'éléments qui doivent être quantifiés « *chaque fois que cela est nécessaire et possible* ».

Les éléments d'un plan préventif de résolution

Aux termes du III de l'article L. 613-38, dix-huit éléments doivent figurer dans un plan préventif de résolution établi par le collège de résolution de l'ACPR :

– un résumé des éléments principaux du plan ;

– un résumé des modifications importantes intervenues à l'intérieur de la personne concernée ou du groupe auquel elle appartient depuis la dernière mise à jour du plan ;

– un descriptif des modalités selon lesquelles les fonctions critiques et les activités fondamentales pourraient être juridiquement et économiquement dissociées des autres fonctions, dans la mesure nécessaire pour assurer leur continuité en cas de défaillance de la personne ou du groupe ;

– un calendrier de mise en œuvre du plan ;

– une description détaillée de l'évaluation ;

– une description de toutes les mesures exigées pour réduire ou supprimer les obstacles signalés à l'issue de l'évaluation ;

– une description des méthodes employées afin de déterminer la valeur et apprécier la cessibilité des branches d'activité exerçant des fonctions critiques, des branches d'activités fondamentales et des actifs de la personne concernée ;

– une description détaillée des dispositions visant à garantir que les informations requises pour établir les plans préventifs de résolution sont à jour et accessibles ;

– une description des modalités de financement des différentes options de résolution, en écartant les hypothèses suivantes : tout soutien financier public exceptionnel à l'exception des concours du fonds de garantie des dépôts et de résolution ou, s'il y a lieu, d'un ou plusieurs autres dispositifs équivalents relevant d'un autre État membre ; tout apport urgent de liquidités par une banque centrale ; tout apport de liquidités par une banque centrale à des conditions non conventionnelles, en termes de constitution de garantie, d'échéance et de taux d'intérêt ;

– une description détaillée des différentes stratégies de résolution susceptibles d'être appliquées en fonction des différents scénarios possibles et des délais applicables ;

– une description des relations d'interdépendance critiques de la personne ou du groupe concerné ;

– une description des différentes options permettant de maintenir l'accès aux systèmes, aux chambres de compensation et aux référentiels centraux, et une évaluation de la portabilité des positions des clients ;

– une analyse de l'incidence du plan sur le personnel de la personne concernée, y compris en termes de coûts, et une description des procédures envisagées en vue de la consultation du personnel au cours du processus de résolution ;

– un plan de communication avec les médias et le public ;

– l'exigence minimale de fonds propres et d'engagements éligibles à laquelle est soumise la personne concernée et, le cas échéant, le délai dans lequel celle-ci se met en conformité avec cette exigence ;

– lorsque le collège de résolution exige qu'une partie de l'exigence minimale soit remplie au moyen de fonds propres ou d'instruments éligibles subordonnés, le calendrier de mise en œuvre de cette exigence par la personne concernée ;

– une description des principaux systèmes et opérations permettant de maintenir le fonctionnement permanent des processus opérationnels de la personne concernée ou du groupe ;

– le cas échéant, tout avis exprimé par la personne concernée ou par le groupe à l'égard du plan préventif de résolution.

Ces dispositions ont été introduites dans le code monétaire et financier par l'article 3 de l'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. Il s'agit d'une transposition de l'article 10 de la directive du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement [1], dite BRRD [2].

2. Le dispositif proposé

L'article 5 (§ 1) de la directive Digital Operational Resilience Act (DORA) du 14 décembre 2022 [3] modifie l'article 10 de la directive BRRD. Il amende deux éléments que les autorités nationales de résolution des États membres doivent faire figurer dans les plans de résolution qu'elles établissent :

– une démonstration de la façon dont les fonctions critiques et les activités fondamentales pourraient être juridiquement et économiquement séparées des autres fonctions dans la mesure nécessaire pour assurer, non seulement leur continuité, mais aussi leur « *résilience opérationnelle numérique* » en cas de défaillance de l'établissement ;

– une description des principaux systèmes et opérations permettant de maintenir en permanence le fonctionnement des processus opérationnels de l'établissement, « *y compris des réseaux et des systèmes d'information visés dans le règlement* [DORA] [4] ».

En conséquence, l'article 54 du projet de loi prévoit de procéder à ces mêmes modifications au sein du III de l'article L. 613-38 du code monétaire et financier, plus précisément au 3° et au 17°.

Concernant la mention des réseaux et des systèmes d'information mis en place et gérés conformément au règlement DORA, cette proposition d'ajout est analogue à celles proposées aux articles 50 et 51 du projet de loi pour les prestataires de services d'investissement [5] .

---

(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 *en anglais.*

(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.

(5) Cf. *commentaires des articles 50 et 51.*

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 55
(art. L. 631-1 du code monétaire et financier)
Extension de la liste des autorités habilitées à échanger des informations

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article modifie l'article L. 631-1 du code monétaire et financier de manière ce que la Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR) soient également habilitées à échanger des informations avec l'Autorité des marchés financiers (AMF) et l'Agence nationale de sécurité des systèmes d'information (ANSSI) dans le domaine de la sécurité des systèmes d'information.

Cette extension est la conséquence de l'application des articles 48 et 49 du règlement DORA du 14 décembre 2022 sur la communication d'informations entre les autorités de surveillance du secteur financier.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code monétaire et financier par l'article 86 de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (loi PACTE).

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

L'article L. 631-1 du code monétaire et financier régit la coopération et les échanges d'information entre les autorités chargées de la surveillance du système financier.

Il institue une coopération entre la Banque de France, ainsi que l'Institut d'émission des départements d'outre-mer (IEDOM) et l'Institut d'émission d'outre-mer (IEOM) qui en émanent, l'ACPR et l'AMF. À ce titre, elles sont habilitées à se communiquer les renseignements utiles à l'accomplissement de leurs missions respectives.

Cette autorisation à échanger des informations concerne aussi d'autres organismes en ce qui concerne des secteurs d'activité spécifiques.

Dans le domaine de pratiques de commercialisation, elle s'applique à l'ACPR, à l'AMF ainsi qu'à l'autorité administrative chargée de la concurrence et de la consommation, en l'espèce la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) du ministère de l'économie, des finances et de la souveraineté industrielle et numérique.

Dans celui de la lutte contre la corruption, le blanchiment des capitaux et le financement du terrorisme, cette faculté concerne l'ACPR, l'administration des douanes ainsi que l'Agence française anticorruption (AFA).

Il existe un troisième domaine dans lequel plusieurs autorités sont autorisées se communiquer les renseignements utiles à l'accomplissement de leurs missions. Il s'agit de la sécurité des systèmes d'information qui concerne l'AMF et l'autorité nationale en charge de la sécurité des systèmes d'information, c'est-à-dire l'ANSSI.

Ce dernier champ d'échange d'informations a été introduit par l'article 86 de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (loi PACTE). Cette disposition était issue d'un amendement en nouvelle lecture de M. Laurent Saint-Martin et de Mme Nadia Hai, députés, visant à ce que l'AMF ne soit pas soumise au secret professionnel lorsqu'elle communique avec l'ANSSI.

2. Le dispositif proposé

L'article 48 du règlement du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier [(1)], dit DORA, pose le principe d'une coopération étroite des autorités compétentes entre elles ainsi qu'avec, le cas échéant, le superviseur principal, c'est-à-dire l'autorité européenne de surveillance.

---

(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.

Son second paragraphe dispose, plus exactement, que « *les autorités compétentes et le superviseur principal s'échangent mutuellement, en temps utile, toutes les informations pertinentes concernant les prestataires tiers critiques de services TIC* [technologies de l'information et de la communication] *qui leur sont nécessaires pour s'acquitter des missions qui leur incombent en vertu du* [règlement DORA]*, en particulier en ce qui concerne les risques recensés, les approches et les mesures adoptées dans le cadre des tâches de supervision du superviseur principal* ».

Quant à l'article 49 (§ 2), il prévoit que les autorités compétentes, les autorités européennes de surveillance et la Banque centrale européenne coopèrent étroitement entre elles et échangent des informations afin de s'acquitter de leurs missions, notamment celle d'imposer des sanctions administratives et des mesures correctives.

Prenant également en compte les nouvelles règles de gestion, de classification et de notification des incidents liés aux TIC pour les entités financières fixées par le chapitre III du règlement DORA [(1)], l'article 55 du projet de loi prévoit d'étendre les échanges d'informations en ce qui concerne la sécurité des systèmes d'information à la Banque de France et à l'ACPR afin d'assurer le respect, d'une part et sous réserve de son adoption par le Parlement, de la loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité et, d'autre part, du règlement DORA.

L'article 55 propose également que cette communication de renseignements utiles à l'exercice des missions respectives de l'AMF, de la Banque de France, de l'ACPR et de l'ANSSI se fasse « *sans délai* ».

Il s'inscrit dans la continuité de l'article 49 du projet de loi qui, dans sa rédaction initiale, limitait à l'ACPR et à la Banque de France l'obligation de déclaration d'incident de paiement prévue à l'article L. 521-10 du code monétaire et financier eu égard à l'application directe du règlement DORA, et notamment son chapitre III, aux prestataires privés de services de paiement. Le présent article entend en tirer les conséquences afin de prévoir des échanges d'information sans délai entre ces deux organismes ainsi que l'AMF et l'ANSSI dans les conditions prévues dans le règlement précité.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

---

(1) Cf. *commentaire de l'article 49.*

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 56

(art. L. 712-7, L. 752-10, L. 753-10, L. 754-8, L. 761-1, L. 762-3, L. 763-3, L. 764-3, L. 762-4, L. 763-4, L. 764-4, L. 771-1, L. 781-1, L. 773-5, L. 774-5, L. 775-5, L. 773-6, L. 774-6, L. 775-6, L. 773-21, L. 774-21, L. 775-15, L. 773-30, L. 774-30, L. 775-24, L. 783-2, L. 784-2, L. 785-2, L. 783-4, L. 784-4, L. 785-4, L. 783-13, L. 784-13 et L. 785-12 du code monétaire et financier)

Adaptations pour rendre applicables en outre-mer les modifications du code monétaire et financier prévues par le présent projet de loi

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article prévoit de rendre applicables aux îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie les dispositions du présent chapitre du projet de loi.

Il étend également l'application du règlement du 14 décembre 2022 relatif à la résilience opérationnelle numérique du secteur financier (DORA) à ces trois territoires ainsi qu'à Saint-Pierre-et-Miquelon en raison de leur statut de pays et régions d'outre-mer associés à l'UE et non de région ultrapériphérique des États membres.

➢ **Dernières modifications législatives intervenues**

Cf. articles 43 à 55 du projet de loi.

➢ **Modifications apportées par le Sénat**

Le Sénat a corrigé plusieurs erreurs de référence, notamment en raison de l'entrée en vigueur de l'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés de crypto-actifs, postérieure à la présentation du projet de loi en conseil des ministres.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement de coordination.

1. L'état du droit

Les articles 43 à 55 du projet de loi prévoient de modifier le code monétaire et financier pour transposer la directive du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (1), dite DORA (2), et l'adapter au règlement éponyme (3).

Conformément à l'article 73 de la Constitution, ces modifications sont applicables de plein droit dans les départements et les régions d'outre-mer, autrement dit en Guadeloupe, en Guyane, en Martinique, à La Réunion et à Mayotte.

L'application dans les collectivités d'outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie dépend des dispositions de la loi organique fixant notamment les conditions dans lesquelles les lois et règlements y sont applicables.

En l'espèce, les articles du chapitre premier du titre III du projet de loi seront également en vigueur dans trois collectivités d'outre-mer sans qu'une mention expresse doive le préciser. Il s'agit de Saint-Barthélemy (4), Saint-Martin (5) et Saint-Pierre-et-Miquelon (6) en application de la loi organique n° 2007-223 du 21 février 2007 portant dispositions statutaires et institutionnelles relatives à l'outre-mer et, plus particulièrement, de l'article L. 711-2 du code monétaire et financier.

En revanche, l'application dans les autres collectivités d'outre-mer régies par l'article 74 et en Nouvelle-Calédonie n'est pas de plein droit et nécessite donc des dispositions spécifiques dans le projet de loi.

L'article L. 711-4 du code précité dispose en effet que « *ne sont applicables en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna que les dispositions du* [code monétaire et financier] *dont l'application est expressément prévue par le* [livre VII : Dispositions relatives à l'outre-mer] », conformément aux statuts respectifs de ces territoires :

– article 4 de la loi n° 61-814 du 29 juillet 1961 conférant aux îles Wallis et Futuna le statut de territoire d'outre-mer ;

---

(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 *en anglais.*

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

(4) Article L. O. 6213-1 du code général des collectivités territoriales.

(5) Article L. O. 6313-1 du même code.

(6) Article L. O. 6413-1 du même code.

– article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie ;

– article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie française.

Enfin, il convient également de rappeler que les règlements de l'Union européenne (UE) ne sont pas d'effet direct dans les pays et territoires d'outre-mer (PTOM) que sont les collectivités d'outre-mer françaises et la Nouvelle-Calédonie, à l'exception de Saint-Martin, contrairement aux régions ultrapériphériques (RUP) qui correspondent, en droit interne, aux départements et régions d'outre-mer mais aussi à Saint-Martin, où le droit de l'UE s'applique de plein droit.

L'article 288 du traité sur le fonctionnement de l'UE stipule que le règlement est directement applicable dans tout État membre. Or l'article 198 du même traité considère les PTOM comme des pays et territoires non européens entretenant « *des relations particulières* » avec plusieurs États membres, donc distincts d'eux, et les place sous un régime d'association avec l'Union et non d'appartenance.

En conséquence, les règlements européens n'ont d'effet direct que dans les départements et régions d'outre-mer et à Saint-Martin.

Toutefois, le règlement DORA est également applicable à Saint-Barthélemy en raison de l'accord monétaire entre l'UE et la France relatif au maintien de l'euro dans cette collectivité d'outre-mer. En effet, l'article L. 712-1 dispose que sont applicables de plein droit les actes juridiques et règles du droit de l'UE nécessaires au bon fonctionnement de l'Union économique et monétaire, notamment relatifs à la prévention de la fraude et de la contrefaçon des moyens de paiement, à la législation bancaire et financière et aux obligations de communication de données statistiques établies par l'Eurosystème.

STATUT DES OUTRE-MER VIS-À-VIS DU DROIT DE L'UE

<table>
<tr><th>Territoire</th><th>Statut en droit interne</th><th>Statut en droit de l'UE</th><th>Effet des règlements européens (cas général)</th><th>Effet du règlement DORA</th></tr>
<tr><td>Guadeloupe</td><td rowspan="5">département et région d'outre-mer (art. 73 de la Constitution)</td><td rowspan="3">Région ultrapériphérique</td><td rowspan="4">Direct</td><td rowspan="3">Direct</td></tr>
<tr><td>Guyane</td></tr>
<tr><td>Martinique</td></tr>
<tr><td>La Réunion</td><td rowspan="4">Pays et territoire d'outre-mer</td></tr>
<tr><td>Mayotte</td></tr>
<tr><td>Saint-Martin</td><td rowspan="5">collectivité d'outre-mer (art. 74)</td><td rowspan="5">Aucun (sauf mention expresse en droit interne)</td></tr>
<tr><td>Saint-Barthélemy</td><td>Direct car champ de la législation bancaire et financière (art. L. 712-1)</td></tr>
<tr><td>îles Wallis et Futuna</td><td rowspan="4">Aucun (sauf mention expresse en droit interne)</td></tr>
<tr><td>Polynésie française</td></tr>
<tr><td>Saint-Pierre-et-Miquelon</td></tr>
<tr><td>Nouvelle-Calédonie</td><td>collectivité sui generis (titre XIII)</td></tr>
</table>

Source : commission spéciale.

2. Le dispositif proposé

L'article 56 prévoit donc de rendre applicables les dispositions du projet de loi aux îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie en intégrant les articles modifiés dans leur rédaction qui résultera du projet de loi dans les différents tableaux dressant une liste des dispositions du code monétaire et financier applicables dans ces trois territoires.

Il prévoit également d'y rendre applicable le règlement DORA ainsi qu'à Saint-Pierre-et-Miquelon en modifiant les articles L. 712-7, L. 761-1, L. 771-1 et L. 781-1 du code monétaire et financier. Ce territoire est en effet un PTOM au sens du traité sur le fonctionnement de l'UE.

3. Les modifications apportées par le Sénat

La commission spéciale a adopté un amendement du rapporteur Michel Canévet corrigeant plusieurs erreurs de référence.

Il supprime la modification des articles L. 761-1, L. 771-1 et L. 781-1 du code monétaire et financier devenue obsolète dans la mesure où ces dispositions font désormais référence au règlement DORA depuis l'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés de crypto-actifs (article 34), date à laquelle le projet de loi a été déposé au Sénat.

L'amendement a également corrigé le renvoi à l'article L. 613-38 (article 54 du projet de loi) pour qu'il s'opère au niveau du tableau figurant à l'article L. 785-3 et non à l'article L. 785-4.

En séance, le Sénat a adopté un autre amendement du rapporteur Michel Canévet corrigeant une autre erreur de ligne dans un tableau avec avis favorable du gouvernement.

4. La position de la commission

La commission spéciale a adopté l'amendement du rapporteur thématique Mickaël Bouloux prévoyant l'application de l'article 49 *bis* en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna et retirant celle de l'article 53 du fait de sa suppression. Il corrige également une erreur de référence.

*

* *

CHAPITRE II
Dispositions modifiant le code des assurances

Article 57
(art. L. 354-1 du code des assurances)
Nouvelles obligations pour les entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article modifie l'article L. 354-1 du code des assurances qui traite des systèmes de gouvernance des entreprises d'assurance et de réassurance mis en place dans le respect des règles prudentielles imposées par la directive du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II).

Il prévoit de faire référence aux règles de gestion et de mise en place des réseaux et systèmes d'information fixées par le règlement DORA du 14 décembre 2022. Il s'agit donc d'une transposition de l'article 2 de la directive du même nom.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code des assurances par l'article 4 de l'ordonnance n° 2015-378 du 2 avril 2015 transposant la directive « solvabilité II ».

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un article rédactionnel.

1. L'état du droit

Les entreprises d'assurance et de réassurance qui relèvent du régime dit solvabilité II sont soumises à plusieurs règles d'ordre prudentiel.

Certaines de ces règles prudentielles ont trait au système de gouvernance que les entreprises d'assurance et de réassurance mettent en place. Ainsi, l'article L. 354-1 prévoit que ce système doit garantir une gestion saine et prudente de l'activité de l'entreprise et faire l'objet d'un réexamen interne régulier. En outre, il doit être proportionné à la nature, à l'ampleur et à la complexité des opérations de l'entreprise.

Le système de gouvernance est tenu de remplir les fonctions suivantes :

– gestion des risques ;

– vérification de la conformité ;

– audit interne ;

– calcul des provisions techniques (fonction actuarielle).

À ce titre, les entreprises soumises à la directive Solvabilité II ont l'obligation d'élaborer et de veiller à la mise en œuvre de politiques écrites relatives, au moins, à la gestion des risques, au contrôle interne, à l'audit interne et, le cas échéant, à l'externalisation.

Elles doivent aussi prendre des dispositions leur permettant d'assurer la continuité et la régularité dans l'exercice de leurs activités, incluant l'élaboration de plans d'urgence au travers notamment de dispositifs, de ressources et de procédures appropriés et proportionnés.

Ces dispositions ont été introduites dans le code des assurances par l'article 4 de l'ordonnance du 2 avril 2015 précitée.

Les entreprises relevant de la directive « solvabilité II »

La seconde directive sur l'accès aux activités de l'assurance et de la réassurance et leur exercice du 25 novembre 2009 (1), dite solvabilité II, impose aux entreprises du secteur de l'assurance de détenir des ressources financières suffisantes et définit des règles de gouvernance, de gestion des risques, de transparence et de contrôle. Elle répond aux normes internationales prudentielles établies par les seconds accords de Bâle pour l'ensemble du secteur financier, dont celui des assurances.

La directive a été transposée en droit interne par l'ordonnance n° 2015-378 du 2 avril 2015.

Les entreprises qui relèvent de son régime sont décrites à l'article L. 310-3-1 du code des assurances :

– les entreprises agréées (2) qui sous forme d'assurance directe contractent des engagements dont l'exécution dépend de la durée de la vie humaine, s'engagent à verser un capital en cas de mariage ou de naissance d'enfants, font appel à l'épargne en vue de la capitalisation en contractant à cet effet des engagements déterminés, couvrent les risques de dommages corporels liés aux accidents et à la maladie ou couvrent d'autres risques y compris ceux liés à une activité d'assistance ;

– les entreprises de réassurance ;

– les succursales des entreprises agréées ;

– les unions entre sociétés d'assurance mutuelles ayant exclusivement pour objet de réassurer intégralement les contrats souscrits par ces dernières.

2. Le dispositif proposé

L'article 2 de la directive DORA du 14 décembre 2022 (3) modifie l'article 41 (§ 4) de la directive Solvabilité II en ce qui concerne les mesures prises par les entreprises d'assurance et de réassurance pour assurer la continuité et la régularité de leurs activités.

(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) Relèvent également de ce régime des entreprises sollicitant un agrément, disposant d'un agrément pour des opérations de responsabilité civile, crédit ou caution ou sans agrément dès lors qu'elles remplissent certaines conditions ayant trait à l'encaissement annuel de primes ou cotisations brutes, au total des provisions techniques, à l'appartenance à un groupe ou encore à la nature de l'activité si elle comporte des opérations de réassurance.

(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.

La directive DORA exige que la mise en place et la gestion de réseaux et de systèmes d'information à ces fins soient conformes aux dispositions du règlement du même nom [(1)].

En conséquence, le **2°** de l'article 57 du projet de loi propose de compléter le quatrième alinéa de l'article L. 354-1 du code des assurances afin de préciser que les entreprises d'assurance et de réassurance mettent en œuvre des dispositifs, 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* [DORA] » afin d'assurer la continuité et la régularité de leurs activités.

Cette modification est analogue à celles proposées aux articles 47, 50, 51 et 54 du projet de loi en ce qui concerne respectivement les établissements de crédit et sociétés de financement, les prestataires de services d'investissement autre que les sociétés de gestion de portefeuille, les sociétés de gestion de portefeuille et les plans préventifs de résolution établis par le collège de résolution de l'Autorité de contrôle prudentiel et de résolution (ACPR) [(2)].

Par ailleurs, le **1°** de l'article 57 propose une modification rédactionnelle du troisième alinéa de l'article L. 354-1 qui prévoit l'élaboration de politiques écrites relatives, entre autres, à l'externalisation. Le projet de loi prévoit qu'il soit précisément fait référence au 13° de l'article L. 310-3, et non plus à l'article dans sa globalité, qui définit l'externalisation comme « *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* ».

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

(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) Cf. *commentaires des articles 47, 50, 51 et 54.*

Article 58

(art. L. 356-18 du code des assurances)

Extension aux groupes d'assurance des nouvelles obligations de gouvernance des risques liés à l'utilisation des systèmes d'information

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article modifie l'article L. 356-18 du code des assurances qui traite des systèmes de gouvernance des groupes mis en place dans le respect des règles prudentielles imposées par la directive du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II).

Il prévoit de faire référence aux règles de gestion et de mise en place des réseaux et systèmes d'information fixées par le règlement DORA du 14 décembre 2022. Il s'agit donc d'une transposition de l'article 2 de la directive du même nom.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code des assurances par l'article 4 de l'ordonnance n° 2015-378 du 2 avril 2015 transposant la directive Solvabilité II.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les règles prudentielles introduites dans le code des assurances par la seconde directive sur l'accès aux activités de l'assurance et de la réassurance et leur exercice du 25 novembre 2009 (1), dite Solvabilité II, s'imposent également aux groupes d'entreprises.

(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.

Le groupe d'entreprises dans le régime Solvabilité II

Aux termes de l'article L. 356-1 du code des assurances, transposant l'article 212 de la directive Solvabilité II, un groupe s'entend alternativement comme :

– un ensemble d'entreprises composé d'une entreprise participante, de ses filiales et des entités dans lesquelles l'entreprise participante ou ses filiales détiennent des participations ainsi que des entités liées du fait que leurs organes d'administration, de direction ou de surveillance sont composés en majorité des mêmes personnes ou qu'elles sont placées sous une direction unique en vertu d'un contrat ou de clauses statutaires ;

– un ensemble d'entreprises fondé sur l'établissement de relations financières fortes et durables, à condition que l'une d'entre elles (l'entreprise mère) exerce effectivement, au moyen d'une coordination centralisée, une influence dominante sur les décisions, y compris les décisions financières, des autres entreprises faisant partie du groupe (les filiales) et que l'établissement et la suppression de ces relations soient soumis à l'approbation préalable du contrôleur du groupe (c'est-à-dire de l'Autorité de contrôle prudentiel et de résolution (ACPR) en application de l'article L. 356-2 du même code).

Les groupes doivent répondre à des exigences spécifiques en matière de système de gouvernance. Elles s'adressent plus particulièrement :

– aux entreprises participantes dans au moins une entreprise d'assurance ou de réassurance, y compris d'un pays tiers ;

– aux entreprises mères prenant la forme d'une société de groupe d'assurance, d'une union mutualiste de groupe, d'une société de groupe assurantiel de protection sociale ou d'une compagnie financière holding mixte.

En application de l'article L. 356-18, ces entreprises participantes et mères sont tenues de mettre en place un système de gouvernance garantissant une gestion saine et prudente de l'activité au niveau du groupe et faisant l'objet d'un réexamen interne régulier. Il doit reposer sur une séparation claire des responsabilités au niveau du groupe et comporte un dispositif efficace de transmission des informations. Ce système de gouvernance est censé être proportionné à la nature, à l'ampleur et à la complexité des opérations du groupe.

Quatre fonctions clés doivent être accomplies par le système de gouvernance des entreprises participantes et mères :

– gestion des risques ;

– vérification de la conformité ;

– audit interne ;

– actuarielle.

Pour ce faire, les entreprises visées doivent élaborer des politiques écrites relatives, au moins, à la gestion des risques, au contrôle interne, à l'audit interne et,

le cas échéant à l'externalisation et veiller à ce qu'elles soient mises en œuvre au niveau du groupe.

Les entreprises participantes et mères ont l'obligation de prendre des dispositions qui leur permettent d'assurer la continuité et la régularité de l'exercice de leurs activités, notamment en établissant des plans d'urgence au niveau du groupe. À cette fin, elles doivent mettre en œuvre des dispositifs, des ressources et des procédures appropriées.

L'ensemble de ces obligations en matière de gouvernance sont analogues à celles imposées aux entreprises d'assurance et de réassurance elles-mêmes à l'article L. 354-1 (1).

Elles ont également été introduites dans le code des assurances par l'article 4 de l'ordonnance du 2 avril 2015 (2) par transposition de l'article 246 de la directive Solvabilité II qui prévoit que les exigences prévues à l'article 41 en matière de système de gouvernance pour les entreprises du secteur de l'assurance s'appliquent *mutatis mutandis* au niveau du groupe.

2. Le dispositif proposé

L'article 2 (§ 1) de la directive DORA du 14 décembre 2022 (3) modifiant l'article 41 (§ 4) de la directive Solvabilité II, dont les dispositions sont étendues au niveau du groupe par l'article 246, l'article 58 du projet de loi prévoit donc une modification similaire de l'article L. 356-18 du code des assurances à celle proposée à l'article L. 354-1.

Ainsi, le **2**° complète le dernier alinéa de l'article L. 356-18 afin de préciser que les entreprises participantes et mères mettent en œuvre des dispositifs, 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* [DORA] (4) » afin d'assurer la continuité et la régularité de leurs activités au niveau du groupe.

Le **1**° prévoit également une modification rédactionnelle du troisième alinéa de l'article L. 356-18 qui prévoit l'élaboration de politiques écrites relatives, entre autres, à l'externalisation. Le projet de loi prévoit qu'il soit précisément fait référence au 13° de l'article L. 310-3, et non plus à l'article dans sa globalité, qui

---

(1) Cf. *commentaire de l'article 57.*

(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 (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.

définit l'externalisation comme « *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* ».

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 58 bis
(art. L. 121-8 du code des assurances)
Inversion de la charge de la preuve pour les cyberattaques

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel adopté par le Sénat prévoit d'inclure les attaques informatiques dans la liste des risques pour lesquels la charge de la preuve pèse sur l'assureur.

Toutefois, la rédaction proposée risque d'impliquer que l'assureur n'est pas tenu d'indemniser les pertes et dommages occasionnés par les cyberattaques dès lors qu'il arrive à en prouver l'origine.

➢ **Dernières modifications législatives intervenues**

L'article L. 121-8 du code des assurances résulte de la codification de l'article 34 de la loi du 13 juillet 1930 (loi Godard) relative au contrat d'assurance par décret en 1976. Il n'a pas été modifié depuis.

➢ **Modifications apportées par la commission**

La commission spéciale a corrigé la rédaction du Sénat de manière à ce que l'assureur ait à prouver qu'une attaque informatique résulte d'une guerre étrangère pour ne pas à avoir à indemniser l'assuré.

1. L'état du droit

L'article L. 121-8 du code des assurances dispose que « *l'assureur ne répond pas, sauf convention contraire, des pertes et dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires* ».

Ces dispositions sont directement issues de l'article 34 de la loi du 13 juillet 1930 relative au contrat d'assurance, dite loi Godard, et figurent dans le code des assurances depuis sa création par décret en 1976 [(1)]. La loi Godard est d'ailleurs considérée comme la première grande loi à régir le droit des assurances terrestres.

Les risques de soulèvements conflictuels et armées, qu'ils prennent la forme d'une guerre ou d'émeutes font ainsi l'objet d'une exclusion assurantielle légale. Sauf mention contraire, la garantie promise par les assureurs dans le cadre de leur couverture n'inclut pas l'indemnisation des dommages subis à la suite de tels événements.

À ce titre, l'article L. 121-8 précise qu'il appartient à l'assureur « *de prouver que le sinistre résulte de la guerre civile, d'émeutes ou de mouvements populaires* ».

En cas de litige sur la qualification de l'origine du sinistre, l'assureur qui invoque l'exclusion voit donc la charge de la preuve peser sur lui. Autrement, dit, il lui revient de démontrer que les dommages en question résultent directement d'une émeute ou d'un mouvement populaire au sens des critères jurisprudentiels.

2. Le dispositif proposé par le Sénat

En séance, le Sénat a adopté un amendement de Mme Vanina Paoli-Gagin insérant un article additionnel après l'article 58 du projet de loi, contre l'avis du gouvernement mais avec l'avis favorable de la commission spéciale.

En cas de cyberattaque, il propose qu'il appartienne à l'assureur de prouver que le sinistre résulte effectivement « *d'attaques informatiques* », à l'instar de ce que l'article L. 121-8 du code des assurances prévoit déjà pour les situations de guerre civile, d'émeutes ou de mouvements populaires.

La sénatrice rappelle qu'il revient à l'assuré de prouver qu'il a été victime d'une cyberattaque. Elle considère qu'« *il lui est quasiment impossible de prouver la cause de ce dommage, compte tenu de la difficulté voire, souvent, de*

(1) Décret n° 76-666 du 16 juillet 1976 relatif à la codification des textes législatifs concernant les assurances.

l'impossibilité d'imputer officiellement une cyberattaque à un acteur en particulier ». Cette charge de la preuve pesant sur l'assuré nuirait au développement de l'assurance des risques cyber en France et favoriserait la concurrence d'entreprises étrangères.

Le gouvernement estime que l'absence d'attractivité des assurances françaises pour la couverture des pertes et dommages occasionnés par les cyberattaques reste à démontrer et craint, au contraire, qu'une telle modification de l'article L. 121-8 les incite à se désengager de ce marché. Une telle inclusion des attaques informatiques à cet article du code des assurances implique que l'assureur n'est pas tenu d'indemniser les sinistres qu'elles occasionnent dès lors qu'il prouve qu'elles en sont bien à l'origine, ce qui irait à l'encontre de l'intention des auteurs de l'amendement.

3. La position de la commission

La commission spéciale a adopté deux amendements identiques du rapporteur général et du rapporteur thématique Mickaël Bouloux visant à corriger la rédaction du Sénat de manière à rendre effective l'inversion de la preuve en cas de cyberattaque.

Ces amendements sont le résultat de travaux conjoints de la direction générale du Trésor, de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) et de la fédération France Assureurs.

Ils prévoient que « *lorsque le sinistre résulte d'une atteinte à un système de traitement automatisé de données au sens des articles 323-1 à 323-8 du code pénal, il appartient à l'assureur de prouver qu'il résulte d'une guerre étrangère* ». Autrement dit, à défaut de pouvoir imputer une cyberattaque à un conflit armé, l'assureur ne peut refuser de répondre des pertes et dommages qu'elle est susceptible d'occasionner.

Par ailleurs, les amendements étendent cette modification dans les îles Wallis et Futuna, collectivité d'outre-mer dans laquelle l'État demeure compétent pour les règles assurantielles.

*

* *

CHAPITRE III
Dispositions modifiant le code de la mutualité

Article 59
(art. L. 211-12 du code de la mutualité)
Nouvelles obligations pour les unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article propose de modifier l'article L. 211-12 du code de la mutualité qui traite des systèmes de gouvernance des mutuelles et unions mis en place dans le respect des règles prudentielles imposées par la directive du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II).

Il prévoit de faire référence aux règles de gestion et de mise en place des réseaux et systèmes d'information fixées par le règlement DORA du 14 décembre 2022. Il s'agit donc d'une transposition de l'article 2 de la directive du même nom.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code de la mutualité par l'article 14 de l'ordonnance n° 2015-378 du 2 avril 2015 transposant la directive Solvabilité II.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les règles prudentielles issues de la seconde directive sur l'accès aux activités de l'assurance et de la réassurance et leur exercice du 25 novembre 2009 (1), dite solvabilité II, ont également été introduites dans le code

(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.

de la mutualité par l'ordonnance du 2 avril 2015 [1], plus précisément par son article 14.

À l'instar des entreprises d'assurance et de réassurance [2], ainsi que de leurs groupes [3], les mutuelles et unions doivent répondre à des exigences spécifiques en matière de système de gouvernance.

En application de l'article L. 211-12 du code de la mutualité, elles sont tenues de 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. Il doit reposer sur une séparation claire des responsabilités au niveau du groupe et comporte un dispositif efficace de transmission des informations. Ce système de gouvernance est censé être proportionné à la nature, à l'ampleur et à la complexité des opérations de la mutuelle ou de l'union.

Quatre fonctions clés doivent être accomplies par leur système de gouvernance :

– la fonction de gestion des risques ;

– la fonction de vérification de la conformité ;

– la fonction d'audit interne ;

– la fonction actuarielle.

Pour ce faire, les mutuelles et les unions doivent élaborer des politiques écrites relatives, au moins, à la gestion des risques, au contrôle interne, à l'audit interne et, le cas échéant, à l'externalisation et veiller à ce que ces politiques soient bien mises en œuvre.

Les mutuelles et les unions ont l'obligation de prendre des dispositions qui leur permettent d'assurer la continuité et la régularité de l'exercice de leurs activités, notamment en établissant des plans d'urgence. À cette fin, elles doivent mettre en œuvre des dispositifs, des ressources et des procédures appropriés.

L'ensemble de ces obligations en matière de gouvernance sont analogues à celles imposées aux entreprises d'assurance et de réassurance [4] ainsi qu'à leurs groupes [5].

---

(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) Cf. *commentaire de l'article 57.*

(3) Cf. *commentaire de l'article 58.*

(4) Article L. 354-1 du code des assurances.

(5) Article L. 356-18 du même code.

Les mutuelles et unions relevant du régime « solvabilité II »

L'article L. 211-10 du code de la mutualité place sous le régime de la directive précitée les mutuelles et les unions ayant pour objet de :

– couvrir les risques de dommages corporels liés à des accidents ou à la maladie ;

– contracter des engagements dont l'exécution dépend de la durée de la vie humaine, verser un capital en cas de mariage ou de naissance d'enfants, faire appel à l'épargne en vue de la capitalisation en contractant des engagements déterminés ;

– réaliser des opérations de protection juridique et d'assistance aux personnes ;

– couvrir le risque de perte de revenus liée au chômage ;

– apporter leur caution mutualiste aux engagements contractés par leurs membres participants en vue de l'acquisition, de la construction, de la location ou de l'amélioration de leur habitat ou de celui de leurs ayants droit.

Ces mutuelles et unions doivent en outre avoir rempli pendant trois exercices annuels consécutifs au moins une condition liée à l'encaissement annuel de cotisations, au total des provisions techniques, à l'appartenance à un groupe d'assurance ou à l'offre d'opérations de réassurance.

Dès lors qu'elles disposent d'un agrément de l'Autorité de contrôle prudentiel et de résolution (ACPR) pour des opérations de caution, les mutuelles et unions entrent dans le champ de la directive même si elles ne remplissent pas une des conditions énoncées ci-avant.

De manière générale, sont également placées sous le régime Solvabilité II les mutuelles et unions qui exercent une activité d'assurance et de réassurance.

2. Le dispositif proposé

L'article 2 (§ 1) de la directive DORA du 14 décembre 2022 [(1)] modifiant l'article 41 (§ 4) de la directive Solvabilité II, l'article 59 du projet de loi prévoit une modification similaire de l'article L. 211-12 du code de la mutualité dans la mesure où les mutuelles et unions ne sont pas distinctes des entreprises d'assurance et de réassurance dans le droit de l'Union européenne.

Ainsi, il est aussi proposé de compléter l'avant-dernier alinéa de l'article L. 211-12 afin de préciser que les mutuelles et les unions mettent en œuvre des dispositifs, des ressources et des procédures appropriés et proportionnés et, en particulier, « *mettent en place et gèrent des réseaux et des systèmes d'information*

(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.

conformément au règlement [DORA] [(1)] » afin d'assurer la continuité et la régularité de leurs activités.

Contrairement aux articles 57 et 58 du projet de loi, il n'est pas nécessaire de corriger, à cette occasion, la référence à l'externalisation, car l'article L. 211-12, dans sa rédaction actuelle, renvoie bien au 13° de l'article L. 310-3 du code des assurances.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

Article 60
(art. L. 212-1 du code de la mutualité)
Suppression de dispositions redondantes dans le code de la mutualité

Adopté par la Commission sans modifications

➢ **Résumé du dispositif et effets principaux**

Cet article tire les conséquences des articles 57 et 59 en prévoyant de ne plus appliquer directement les dispositions de l'article L. 354-1 du code des assurances aux mutuelles et unions relevant du régime de la directive Solvabilité II du 25 novembre 2009.

En effet, l'article 57 transpose l'article 2 de la directive DORA du 14 décembre 2022 pour insérer à l'article L. 354-1 du code des assurances la référence au règlement éponyme en ce qui concerne les réseaux et systèmes d'information dans le système de gouvernance des entreprises d'assurance et de réassurance. L'article 59 réplique ces mêmes modifications pour les mutuelles et les unions à l'article L. 211-12 du code de la mutualité. Dès lors, l'exclusion de l'application directe de l'article L. 354-1 du code des assurances aux mutuelles et

(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.

unions par l'article L. 212-1 du code de la mutualité permettrait d'éviter une redondance.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code de la mutualité par l'article 15 de l'ordonnance du 2 avril 2015 transposant la directive Solvabilité II.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale n'a pas modifié cet article.

1. L'état du droit

Les règles prudentielles transposées en droit interne à partir de la seconde directive sur l'accès aux activités de l'assurance et de la réassurance et leur exercice du 25 novembre 2009 (1), dite Solvabilité II, s'appliquent également aux mutuelles et aux unions (2), notamment à celles qui pratiquent des opérations d'assurance et de capitalisation ainsi que les mutuelles et unions de retraite professionnelle supplémentaire.

L'article L. 212-1 du code de la mutualité précise que les règles prudentielles applicables aux entreprises d'assurance et de réassurance relevant du régime Solvabilité II (3) s'appliquent également aux mutuelles et unions placées sous ce même régime. Il leur étend aussi les dispositions de l'article L. 310-12-4 du code des assurances qui traite de l'examen et de l'évaluation, par l'Autorité de contrôle prudentiel et de résolution (ACPR) des stratégies, des processus et des procédures de communication d'information établis par les entreprises d'assurance et de réassurance.

L'extension de ces dispositions du code des assurances aux mutuelles et aux unions a été introduite dans le code de la mutualité par l'article 15 de l'ordonnance du 2 avril 2015 (4) de transposition de la directive Solvabilité II.

---

(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) Cf. *commentaire de l'article 59.*

(3) Titre V du livre III du code des assurances.

(4) 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. Le dispositif proposé

Le titre V du livre III du code des assurances comprend l'article L. 354-1 sur la mise en place d'un système de gouvernance par les entreprises d'assurance et de réassurance dans le respect des règles prudentielles du régime Solvabilité II [(1)].

Dès lors, la transposition de l'article 2 (§ 1) de la directive DORA du 14 décembre 2022 [(2)], modifiant l'article 41 (§ 4) de la directive Solvabilité II, proposée par l'article 59 du projet de loi entraîne une redondance dans le code de la mutualité. En effet, l'article L. 211-12 ainsi modifié imposerait que les mutuelles et unions assurent la continuité et la régularité de leurs activités en mettant en place et en gérant des réseaux et systèmes d'information conformément aux exigences du règlement DORA [(3)] par similarité avec l'article L. 354-1 du code des assurances dont la modification est proposée par l'article 57 du projet de loi.

En conséquence, le présent article propose d'exclure l'application directe de ces dispositions du code des assurances aux mutuelles et unions relevant du régime Solvabilité II.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté cet article sans le modifier.

*

* *

(1) Cf. *commentaire de l'article 57.*

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

CHAPITRE IV
Dispositions modifiant le code de la sécurité sociale

Article 61
(art. L. 931-7 du code de la sécurité sociale)
Nouvelles obligations pour les institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article modifie l'article L. 931-7 du code de la sécurité sociale qui traite des systèmes de gouvernance des institutions de prévoyance et unions mis en place dans le respect des règles prudentielles imposées par la directive du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II).

Il prévoit de faire référence aux règles de gestion et de mise en place des réseaux et systèmes d'information fixées par le règlement DORA du 14 décembre 2022. Il s'agit donc d'une transposition de l'article 2 de la directive du même nom.

➢ **Dernières modifications législatives intervenues**

Ces dispositions ont été introduites dans le code de la mutualité par l'article 17 de l'ordonnance n° 2015-378 du 2 avril 2015 transposant la directive Solvabilité II.

➢ **Modifications apportées par le Sénat**

Cet article n'a pas été modifié par le Sénat.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement rédactionnel.

1. L'état du droit

Les règles prudentielles issues de la seconde directive sur l'accès aux activités de l'assurance et de la réassurance et leur exercice du 25 novembre 2009 (1), dite Solvabilité II, ont également été introduites dans le code

(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.

de la sécurité sociale par l'ordonnance du 2 avril 2015 [1], plus précisément par son article 17. Elles concernent les institutions de prévoyance et les unions.

À l'instar des entreprises d'assurance et de réassurance [2], ainsi que de leurs groupes [3], et des mutuelles et unions [4], les institutions de prévoyance et leurs unions doivent répondre à des exigences spécifiques en matière de système de gouvernance.

En application de l'article L. 931-7 du code de la sécurité sociale, elles sont tenues de 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. Il doit reposer sur une séparation claire des responsabilités et comporter un dispositif efficace de transmission des informations. Ce système de gouvernance est censé être proportionné à la nature, à l'ampleur et à la complexité des opérations de l'institution de prévoyance ou de l'union.

Les institutions de prévoyance et unions relevant du régime Solvabilité II

L'article L. 931-6 du code de la sécurité sociale place sous le régime de la directive précitée les institutions de prévoyance et les unions ayant pour objet de :

– contracter des engagements dont l'exécution dépend de la durée de la vie humaine, verser un capital en cas de mariage ou de naissance d'enfants, faire appel à l'épargne en vue de la capitalisation en contractant des engagements déterminés ;

– couvrir les risques de dommages corporels liés à des accidents ou à la maladie ;

– couvrir le risque chômage.

Ces institutions de prévoyance et unions doivent en outre avoir rempli pendant trois exercices annuels consécutifs au moins une condition liée à l'encaissement annuel de cotisations, au total des provisions techniques, à l'appartenance à un groupe d'assurance ou à l'offre d'opérations de réassurance.

De manière générale, sont également placées sous le régime Solvabilité II les institutions de prévoyance et unions qui exercent une activité d'assurance et de réassurance.

Quatre fonctions clés doivent être accomplies par leur système de gouvernance :

– la fonction de gestion des risques ;

---

(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) Cf. *commentaire de l'article 57.*

(3) Cf. *commentaire de l'article 58.*

(4) Cf. *commentaire de l'article 59.*

– la fonction de vérification de la conformité ;

– la fonction d'audit interne ;

– la fonction actuarielle.

Pour ce faire, les institutions de prévoyance et les unions doivent élaborer des politiques écrites relatives, au moins, à la gestion des risques, au contrôle interne, à l'audit interne et, le cas échéant, à l'externalisation et veiller à ce que ces politiques soient bien mises en œuvre.

Les institutions de prévoyance et les unions ont l'obligation de prendre des dispositions qui leur permettent d'assurer la continuité et la régularité de l'exercice de leurs activités, notamment en établissant des plans d'urgence. À cette fin, elles doivent mettre en œuvre des dispositifs, des ressources et des procédures appropriés.

L'ensemble de ces obligations en matière de gouvernance sont analogues à celles imposées aux entreprises d'assurance et de réassurance (1), à leurs groupes (2) et aux mutuelles et unions (3).

2. Le dispositif proposé

L'article 2 (§ 1) de la directive DORA du 14 décembre 2022 (4) modifiant l'article 41 (§ 4) de la directive Solvabilité II, l'article 61 du projet de loi prévoit une modification similaire de l'article L. 931-7 du code de la sécurité sociale dans la mesure où les institutions de prévoyance et unions ne sont pas distinctes des entreprises d'assurance et de réassurance dans le droit de l'Union européenne.

Ainsi, il est aussi proposé de compléter l'avant-dernier alinéa de l'article L. 931-7 afin de préciser que les institutions de prévoyance et les unions mettent en œuvre des dispositifs, 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* [DORA] (5) » afin d'assurer la continuité et la régularité de leurs activités.

---

(1) Article L. 354-1 du code des assurances.

(2) Article L. 356-18 du même code.

(3) Article L. 211-12 du code de la mutualité.

(4) 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.

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

Contrairement aux articles 57 et 58 du projet de loi, il n'est pas nécessaire de corriger, à cette occasion, la référence à l'externalisation, l'article L. 931-7, dans sa rédaction actuelle, renvoie bien au 13° de l'article L. 310-3 du code des assurances.

3. Les modifications apportées par le Sénat

Le Sénat n'a pas modifié cet article.

4. La position de la commission

La commission spéciale a adopté l'amendement rédactionnel du rapporteur thématique Mickaël Bouloux.

*

* *

CHAPITRE V
Dispositions finales

Article 62 A
Absence de double assujettissement à DORA et NIS 2

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel adopté par le Sénat prévoit d'exclure expressément du champ de la nouvelle directive NIS 2 les entités financières auxquelles s'appliquent le règlement et la directive DORA en ce qui concerne les mesures de gestion des risques en matière de cybersécurité ou de notification d'incidents importants.

➢ **Dernières modifications législatives intervenues**

La transposition dans le droit interne des directives NIS 2 et DORA, publiées le 14 décembre 2022, fait respectivement l'objet des titres II et III du projet de loi.

➢ **Modifications apportées par la commission**

La commission spéciale a adopté un amendement étendant l'application de cet article en outre-mer et corrigeant une erreur de référence.

1. L'état du droit

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 européenne (UE) [(1)], dite NIS 2, est l'objet du titre II du projet de loi [(2)].

Pour rappel, la directive NIS 2 élargit de manière très importante le champ des acteurs et secteurs régulés au titre du renforcement de la cybersécurité des entités qualifiées comme essentielles ou importantes en raison des services qu'elles fournissent et de leur taille. Plus exactement, la nouvelle directive vise les secteurs et les types d'entités qui ont le plus grand impact potentiel sur l'économie et la société.

L'entrée en vigueur des dispositions du titre II du projet de loi devrait multiplier par trente le nombre d'entités soumises à régulation (environ 15 000 contre 500 à présent) et par trois celui des secteurs régulés (18 contre 6).

Dès lors se pose la question d'un double assujettissement des entités financières visées par le règlement du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier [(3)] (DORA) et la directive éponyme [(4)] dont le titre III du projet de loi entend assurer la transposition dans le droit interne en modifiant principalement le code monétaire et financier [(5)] mais aussi le code des assurances [(6)], le code de la mutualité [(7)] et le code de la sécurité sociale [(8)].

Quant à la directive NIS 2, elle s'adresse aux entités publiques ou privées qui relèvent de secteurs hautement critiques, dont ceux de la banque, des infrastructures des marchés financiers et de la gestion des services TIC interentreprises, en application de son article 2 et de l'annexe I.

Néanmoins, l'article 4 de la directive NIS 2 traite du risque de chevauchement de son champ avec celui des actes DORA. Il dispose 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*

---

(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.

(2) Cf. *commentaires des articles 5 à 42.*

(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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.

(4) 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.

(5) Cf. *commentaires des articles 43 A à 56.*

(6) Cf. *commentaires des articles 57 à 58* bis.

(7) Cf. *commentaires des articles 59 à 60.*

(8) Cf. *commentaire de l'article 61.*

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 NIS 2]*, les dispositions pertinentes de* [cette même directive] *ne sont pas applicables auxdites entités* ». Or, en application de son article 1er (§ 2), le règlement DORA est expressément considéré comme un acte juridique sectoriel *« 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] ».

En conséquence, les entités financières qui auraient été susceptibles d'être soumises aux obligations de la directive NIS 2 n'auront pas, dans la plupart des cas, à s'y conformer dans la mesure où le règlement et la directive DORA prévoient des exigences équivalentes, notamment pour ce qui concerne la gestion du risque lié aux TIC. À l'inverse, l'obligation d'enregistrement des noms de domaine prévue au chapitre V de la directive NIS 2 s'appliquera bien aux entités financières, faute de trouver un équivalent dans les actes DORA.

Le champ d'application du règlement et de la directive DORA

L'article 2 du règlement DORA dispose qu'il s'applique aux entités suivantes :

– les établissements de crédit ;

– les établissements de paiement ;

– les prestataires de services d'information sur les comptes ;

– les établissements de monnaie électronique ;

– les entreprises d'investissement ;

– les prestataires de services du crypto-actifs agréés et les émetteurs de jetons se référant à un ou des actifs ;

– les dépositaires centraux de titres ;

– les contreparties centrales ;

– les plates-formes de négociation ;

– les référentiels centraux ;

– les gestionnaires de fonds d'investissement alternatifs ;

– les sociétés de gestion ;

– les prestataires de services de communication de données ;

– les entreprises d'assurance et de réassurance ;

– les intermédiaires d'assurance, de réassurance et d'assurance à titre accessoire ;

– les institutions de retraite professionnelle ;

– les agences de notation de crédit ;

– les administrateurs d'indices de référence d'importance critique ;

– les prestataires de services de financement participatif ;

– les référentiels de titrisation ;

– les prestataires tiers de services de technologies de l'information et de la communication (TIC).

À l'exception de ces derniers, le règlement dénomme « entités financières » l'ensemble de ces acteurs.

Malgré la reconnaissance de ce principe de *lex specialis*, des interrogations demeurent.

Premièrement, l'article 4 de la directive NIS 2 dispose aussi 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 NIS 2]*, les dispositions pertinentes* [de la directive NIS 2] *continuent de s'appliquer aux entités non couvertes par ces actes juridiques sectoriels de l'Union* ». Se pose ainsi la question de l'entrée des entreprises d'assurance dans le champ de la directive NIS 2 comme le soulève la Commission supérieure du numérique et des postes (CSNP) dans son avis du 3 octobre 2024 présenté par M. Damien Michallet, sénateur, et la rapporteure Mme Anne Le Hénanff [(1)].

Deuxièmement, la notion d'équivalence des effets des exigences prévues par les actes DORA par rapport aux obligations de la directive NIS 2 reste difficile à appréhender, notamment dans l'attente de la publication par la Commission européenne des actes d'exécution d'une part et de la publication par le gouvernement des actes réglementaires consécutifs à l'entrée en vigueur du présent projet de loi, ce qui suscite l'inquiétude des représentants des entités auditionnées par le rapporteur Mickaël Bouloux. Le débat autour de l'équivalence de l'obligation de déclaration des incidents majeurs liés aux TIC et de la notification volontaire des cybermenaces importantes par les entités financières, prévue à l'article 19 du règlement DORA, par rapport à l'obligation d'information, prévue à l'article 23 de la directive NIS 2, et à la notification volontaire d'informations pertinentes (article 30) en est une illustration [(2)].

2. Le dispositif proposé par le Sénat

La commission spéciale a adopté un amendement du rapporteur Michel Canévet insérant un article additionnel au projet de loi afin d'éviter explicitement tout risque de double assujettissement entre les deux actes législatifs européens et de lever toute ambiguïté concernant le niveau d'équivalence de leurs exigences respectives.

Il prévoit que les entités financières essentielles et importantes auxquelles s'applique le titre III du projet de loi et auxquelles s'impose l'adoption de mesures de gestion des risques en matière de cybersécurité ou la notification d'incidents importants, conformément au règlement DORA, 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* ».

---

(1) CSNP, avis n° 2024-07 du 3 octobre 2024, Les enjeux de la transposition de la directive NIS 2 en France.

(2) Cf. *commentaires des articles 43 A et 45* bis.

En séance, l'article additionnel a été adopté sans faire l'objet d'aucun amendement, y compris de la part du gouvernement.

3. La position de la commission

La commission spéciale a adopté l'amendement du rapporteur général corrigeant une erreur de référence et prévoyant l'application des dispositions de l'article 62 A en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

*

* *

Article 62
Dates d'application des dispositions du titre III

Adopté par la Commission avec modifications

➢ **Résumé du dispositif et effets principaux**

Dans sa rédaction initiale, l'article 62 prévoyait une entrée en vigueur des dispositions du titre III à compter du 17 janvier 2025 comme le fixait l'article 9 de la directive DORA du 14 décembre 2022.

Concernant l'application des articles 46, 47 et 54 (nouvelles exigences prudentielles imposées aux prestataires de services bancaires), le projet de loi accordait un délai supplémentaire d'un an pour les sociétés de financement de petite taille et non complexes, celles-ci n'étant pas formellement visées par la directive.

➢ **Dernières modifications législatives intervenues**

(sans objet)

➢ **Modifications apportées par le Sénat**

En commission, les sénateurs ont modifié l'article 62 de manière à prévoir une entrée en vigueur des dispositions du titre III, dans leur ensemble, le lendemain de la promulgation de la loi.

Pour la totalité des sociétés de financement, les articles 46, 47 et 54 ne seraient applicables qu'au 1er janvier 2030.

En séance, le Sénat a également prévu que les règles relatives à la gestion des risques et incidents liés aux TIC, à la réalisation des tests de résilience opérationnelle numérique ainsi qu'au respect des principes clés pour une bonne

gestion des risques liés aux prestataires tiers de services TIC, prévues par le règlement DORA, ne soient applicables aux sociétés de financement de petite taille et non complexes que dans le respect d'un principe de proportionnalité.

Les modifications relatives aux sociétés de financement ont reçu un avis défavorable du gouvernement.

➢ **Modifications apportées par la commission**

La commission spéciale a réintroduit une entrée en application différenciée des articles 46, 47 et 54 selon la taille des sociétés de financement : dès le lendemain de la promulgation de la loi pour les plus importantes et le 17 janvier 2027 pour celles de petite taille et non complexes.

1. L'état du droit

L'article 9 de la directive du 14 décembre 2022 concernant la résilience opérationnelle numérique du secteur financier [(1)] (DORA) fixe au 17 janvier 2025 la date limite de transposition dans le droit interne des États membres, soit un délai de pratiquement deux ans depuis sa publication au Journal officiel de l'Union européenne (UE).

Le projet de loi, dont le titre III transpose la directive DORA, a été présenté en conseil des ministres et déposé au Sénat le 15 octobre 2024 par le premier ministre Michel Barnier.

Quant au Conseil d'État, il a été saisi dès le 7 mai 2024 et a rendu son avis le 6 juin 2024, ce qui laisse à penser que le projet de loi aurait probablement été présenté plus tôt au Parlement si la dissolution de l'Assemblée nationale par le président de la République le 9 juin 2024 n'était pas intervenue.

2. Le dispositif proposé

L'article 62 de la version initiale du projet de loi proposait que les dispositions du titre III soient applicables à compter du 17 janvier 2025, comme le prévoyait l'article 9 de la directive DORA.

Il entendait toutefois accorder un délai supplémentaire aux sociétés de financement les plus petites pour l'application des articles 46, 47 et 54 du projet de loi.

Les sociétés de financement appartiennent à la catégorie des prestataires de service bancaires avec les établissements de crédit. Elles constituent des personnes morales, autres que ces derniers, qui effectuent à titre de profession habituelle et

(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.

pour leur propre compte des opérations de crédit dans les conditions et limites définies par leur agrément [1]. La principale différence par rapport aux établissements de crédit est qu'elles ne peuvent pas recevoir des fonds remboursables du public, à l'instar des dépôts.

Les entreprises de crédit-bail mobilier et immobilier, les sociétés de caution mutuelle et l'Agence française de développement (AFD) sont des exemples de sociétés de financement.

Pour rappel, l'article 46 met en cohérence les exigences prudentielles auxquelles sont soumis les prestataires de services bancaires avec la prise en compte renforcée du risque lié aux technologies de l'information et de la communication (TIC) par le règlement DORA [2].

L'article 47 oblige ces mêmes prestataires à se doter d'un dispositif de gouvernance solide de manière à inclure les réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA.

Quant à l'article 54, il prévoit que les plans de résolution établis par le collège de résolution de l'Autorité de contrôle prudentiel et de résolution (ACPR) fassent bien référence à la résilience opérationnelle numérique ainsi qu'aux réseaux et aux systèmes d'information mis en place et gérés conformément au règlement DORA.

Comme indiqué dans les commentaires des articles 46 et 47, la directive DORA, en modifiant la directive sectorielle CRD du 26 juin 2013 [3], ne vise que les établissements de crédit et non les sociétés de financement. Le gouvernement a néanmoins fait le choix d'étendre à ces dernières la transposition de la directive dans la mesure où « *ces sociétés sont confrontées aux mêmes risques en matière de sécurité des systèmes d'information* » comme le souligne le Conseil d'État dans son avis sur le projet de loi. Il faut d'ailleurs rappeler que les dispositions prudentielles du code monétaire et financier (article L. 511-41 et suivants) traitent les sociétés de financement de la même manière que les établissements de crédit.

Toutefois, le gouvernement a souhaité leur accorder un délai de mise en œuvre supplémentaire lorsqu'elles sont de petite taille et non complexes et que leurs moyens et ressources sont réputés moins importantes, autrement dit lorsqu'elles

(1) Article L. 511-1 du code monétaire et 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) 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.

remplissent les conditions prévues à l'article 4 (§ 1) du règlement CRR (*Capital Requirements Regulation*) [1] auquel la directive CRD est associée.

À l'inverse, les sociétés de financement qui ne remplissent pas ces conditions devraient appliquer les dispositions de la directive DORA modifiant la directive CRD dont la transposition dans le code monétaire et financier est proposée aux articles 46, 47 et 54 du projet de loi.

(1) 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.

Les établissements de petite taille et non complexes au sens du règlement CRR

Le point 145 du paragraphe 1 de l'article 4 du règlement CRR du 26 juin 2013, dans sa version en vigueur modifiée par deux règlements du 20 mai 2019 (1) et du 31 mai 2024 (2) fixe les conditions suivantes pour qu'un établissement soit considéré comme « de petite taille et non complexe » :

– il ne s'agit pas d'un établissement de grande taille ;

– la valeur totale de ses actifs sur base individuelle ou, le cas échéant, sur base consolidée est en moyenne égale ou inférieure à un seuil de 5 milliards d'euros sur la période de quatre ans qui précède immédiatement la période de déclaration annuelle en cours ;

– il n'est soumis à aucune obligation, ou est soumis à des obligations simplifiées, en ce qui concerne la planification des mesures de redressement et de résolution ;

– son portefeuille de négociation est classé comme étant de faible taille ;

– la valeur totale de ses positions sur les instruments dérivés qu'il détient à des fins de négociation ne dépasse pas 2 % du montant total de ses actifs au bilan et hors bilan et la valeur totale de l'ensemble de ses positions sur instruments dérivés ne dépasse pas 5 % ;

– les actifs ou les passifs consolidés de l'établissement liés à des activités avec des contreparties situées dans l'Espace économique européen (EEE), à l'exclusion des expositions intragroupe dans l'EEE, dépassent 75 % du total des actifs et des passifs consolidés de l'établissement, à l'exclusion, dans les deux cas, des expositions intragroupe ;

– l'établissement n'utilise pas de modèles internes pour satisfaire aux exigences prudentielles prévues par le règlement CRR, à l'exception des filiales qui utilisent des modèles internes mis au point au niveau du groupe, à condition que ce groupe soit soumis aux exigences de publication sur base consolidée ;

– l'établissement n'a pas communiqué à l'autorité compétente son opposition à être classé en tant qu'établissement de petite taille et non complexe ;

– l'autorité compétente n'a pas jugé, sur la base d'une analyse de la taille, de l'interconnexion, de la complexité ou du profil de risque de l'établissement, que l'établissement ne doit pas être considéré comme étant un établissement de petite taille et non complexe.

3. Les modifications apportées par le Sénat

a. En commission

La commission spéciale a adopté un amendement du rapporteur Michel Canévet repoussant l'entrée en vigueur des dispositions du titre III du projet de loi :

– au lendemain de la promulgation de la loi (au lieu du 17 janvier 2025) de manière générale ;

– au 1er janvier 2030 pour l'application des articles 46, 47 et 54 (au lieu du 17 janvier 2026) à l'ensemble des sociétés de financement et non plus seulement à celles considérées comme des établissements de petite taille et non complexes.

Le report au lendemain de la promulgation tient compte du retard pris dans l'examen du projet de loi. L'adoption d'une motion de censure par l'Assemblée nationale le 4 décembre 2024, suite à l'engagement de la responsabilité du gouvernement sur le vote du projet de loi de financement de la sécurité sociale pour 2025 conformément à l'article 49, alinéa 3, de la Constitution a entraîné la démission du gouvernement.

L'entrée en fonction d'un nouveau gouvernement dirigé par le premier ministre François Bayrou le 13 décembre et l'adoption définitive des projets de loi de finances et de financement de la sécurité sociale pour 2025 au mois de février ont conduit à retarder l'examen du présent projet de loi.

La commission spéciale du Sénat n'a adopté le texte que le 4 mars 2025, soit plus d'un mois après la date prévue par la directive DORA et la version initiale de l'article 62.

Concernant les sociétés de financement, le rapporteur considère l'application des nouvelles exigences prudentielles apportées par la directive DORA comme une « surtransposition » dans la mesure où la directive CRD qu'elle amende ne vise que les établissements de crédit et les entreprises d'investissement. Selon lui, une telle extension est « *susceptible de désavantager les entreprises françaises par rapport à des entreprises européennes de statut équivalent* ».

b. En séance

Le gouvernement a présenté un amendement afin de rétablir une entrée en application des articles 46, 47 et 54 aux seules sociétés de financement de petite taille et non complexes à compter du 17 janvier 2026. Pour les autres dispositions, l'amendement rejoignait la position de la commission spéciale visant à prévoir une entrée en vigueur le lendemain de la promulgation du projet de loi.

Lors de la discussion en séance, la ministre a jugé que « *le 1er janvier 2030 apparaît comme un horizon trop lointain, compte tenu du développement* [des

---

(1) Règlement (UE) 2019/876 du Parlement européen et du Conseil du 20 mai 2019 modifiant le règlement (UE) n° 575/2013 en ce qui concerne le ratio de levier, le ratio de financement stable net, les exigences en matière de fonds propres et d'engagements éligibles, le risque de crédit de contrepartie, le risque de marché, les expositions sur contreparties centrales, les expositions sur organismes de placement collectif, les grands risques et les exigences de déclaration et de publication, et le règlement (UE) n° 648/2012.

(2) Règlement (UE) 2024/1623 du Parlement européen et du Conseil du 31 mai 2024 modifiant le règlement (UE) n° 575/2013 en ce qui concerne les exigences pour risque de crédit, risque d'ajustement de l'évaluation de crédit, risque opérationnel et risque de marché et le plancher de fonds propres.

cyberattaques] » et que « *l'ampleur de cette différenciation est inéquitable par rapport à d'autres acteurs du secteur financier distribuant des services comparables aux sociétés de financement* ». Le gouvernement considère en effet que les sociétés de financement de grande taille exercent des activités critiques pour le secteur financier et doivent être soumises, comme les établissements de crédit, aux exigences prudentielles prévues par la directive CRD modifiée par la directive DORA. Quant aux sociétés de financement de petite taille et non complexes, le délai accordé pour qu'elles puissent se mettre en conformité doit demeurer proportionné à l'objectif poursuivi.

Les sénateurs ont rejeté l'amendement du gouvernement et adopté un nouvel amendement du rapporteur Michel Canévet, contre l'avis du gouvernement. Celui-ci complète la rédaction de la commission spéciale d'un second alinéa disposant que lorsque les sociétés de financement sont de petite taille et non complexes, elles « *appliquent les règles énoncées aux chapitres II à IV et à la section 1 du chapitre V du règlement* [DORA] *conformément au principe de proportionnalité énoncé à l'article 4 du même règlement* ».

Les chapitres et sections du règlement DORA mentionnées par l'amendement portent respectivement sur :

– la gestion du risque lié aux TIC ;

– la gestion, la classification et la notification des incidents liés aux TIC ;

– les tests de résilience opérationnelle numérique ;

– les principes clés pour une bonne gestion des risques liés aux prestataires tiers de services TIC.

L'auteur de l'amendement souhaite donc aller plus loin que la version du texte adopté en commission spéciale dans la mesure où non seulement l'ensemble des sociétés de financement ne seraient tenues d'appliquer les dispositions d'ordre prudentiel de la directive DORA (articles 46, 47 et 54 du projet de loi) qu'à compter du 1er janvier 2030, mais qu'en plus les sociétés de financement de petite taille et non complexes n'appliqueraient que de manière incomplète l'ensemble des autres dispositions du titre III au nom du principe de proportionnalité.

L'article 4 du règlement DORA prévoit que les entités financières mettent en œuvre les règles énoncées au chapitre et sections évoquées ci-avant « *conformément au principe de proportionnalité, en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations* ».

Pour le rapporteur Michel Canévet, l'objectif est de « *modérer les effets de la surtransposition née de la soumission des sociétés de financement au règlement DORA* […] *tout en préservant la pleine application dudit règlement pour les sociétés de financement systémiques* ».

4. La position de la commission

La commission spéciale a adopté les amendements identiques du rapporteur général et du rapporteur thématique Mickaël Bouloux visant à revenir sur le délai d'application au 1er janvier 2030 pour toutes les sociétés de financement.

Le rapporteur thématique a rappelé que les sociétés de financement les plus importantes ne sont qu'une dizaine et que la plus sensible est le Crédit Logement tandis que les sociétés considérées comme de petite taille et non complexes au sens du règlement CRR constituent la très grande majorité (135 entreprises agréées). Dans ce contexte, il a estimé qu'un délai différé au 1er janvier 2030 était excessif au regard des enjeux en matière de résilience opérationnelle numérique et injustifié pour les grandes sociétés de financement.

Les amendements adoptés visent donc à rétablir un délai différencié pour l'entrée en application des articles 46, 47 et 54 du projet de loi :

– le 17 janvier 2027 pour les sociétés de financement de petite taille et non complexes ;

– le lendemain de la promulgation de la loi pour les autres.

La date du 17 janvier 2027 est postérieure d'un an à celle qui figurait dans la version initiale du projet de loi et tient ainsi compte de la particularité des sociétés de financement les plus petites.

La commission spéciale a, en revanche, maintenu le principe de proportionnalité introduit par le Sénat.

COMPARAISON DES VERSIONS DE L'ARTICLE 62

<table>
<tr><th></th><th rowspan="2">Entrée en vigueur du titre III dans son ensemble</th><th colspan="2">Entrée en application des articles 46, 47 et 54</th></tr>
<tr><th>Établissements de crédit</th><th>Sociétés de financement</th></tr>
<tr><td>Projet de loi initial</td><td colspan="2">17 janvier 2025</td><td>17 janvier 2026

(pour les sociétés de financement de petite taille et non complexes au sens du règlement CRR)</td></tr>
<tr><td>Texte adopté par la commission spéciale du Sénat</td><td colspan="2">Lendemain de la promulgation</td><td rowspan="2">1er janvier 2030
(pour toutes les sociétés de financement)</td></tr>
<tr><td>Texte adopté par le Sénat</td><td rowspan="2">Lendemain de la promulgation

mais

Principe de proportionnalité pour l'application des chapitres II, III, IV et V (section 1) du règlement DORA pour les sociétés de financement de petite taille et non complexes au sens du règlement CRR</td><td rowspan="2">Lendemain de la promulgation</td></tr>
<tr><td>Texte adopté par la commission spéciale de l'Assemblée nationale</td><td>17 janvier 2027

(pour les sociétés de financement de petite taille et non complexes au sens du règlement CRR)</td></tr>
</table>

Source : commission spéciale.

La commission spéciale a également adopté l'amendement du rapporteur général étendant l'application de cet article en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

*

* *

Article 63 (nouveau)

Demande de rapport sur les moyens humains et financiers de l'Agence nationale de la sécurité des systèmes d'information

Introduit par la Commission spéciale

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel vise à ce que le gouvernement remette un rapport au Parlement sur les moyens que nécessiterait l'Agence nationale de sécurité des systèmes d'information (ANSSI) pour mettre en œuvre les dispositions du titre II du projet de loi.

➢ **Dernières modifications législatives intervenues**

(sans objet).

1. L'état du droit

L'Agence nationale pour la sécurité des systèmes d'information (ANSSI) a été créée par décret en juillet 2009 (1). Elle est rattachée au secrétariat général de la défense et de la sécurité nationale (SGDSN) et fait ainsi partie des services du Premier ministre.

Les crédits destinés à l'ANSSI sont regroupés au sein du programme 129 *Coordination du travail gouvernemental* de la mission *Direction de l'action du Gouvernement*.

En 2024, l'ANSSI disposait d'un budget de 29,6 millions d'euros (hors dépenses de personnel) et employait 656 agents dont 85,3 % de contractuels.

Les documents annexés au projet de loi de finances pour 2025 (2) prévoyaient d'ailleurs une augmentation de 0,6 millions d'euros en autorisations d'engagement (AE) et de 1,3 million d'euros d'euros en crédits de paiement (CP) pour le pilotage national de la politique de sécurité des systèmes d'information par

(1) 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 ».

(2) Projet annuel de performances de la mission Direction de l'action du Gouvernement *annexé au projet de loi de finances pour 2025.*

rapport à l'année précédente en raison notamment des missions nouvelles liées à la transposition en droit interne de la directive NIS 2 [(1)].

Les missions de l'ANSSI

En application de l'article 3 du décret portant sa création, l'ANSSI est chargée :

– d'assurer la fonction d'autorité nationale de défense des systèmes d'information, notamment en proposant au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et en coordonnant, dans le cadre des orientations fixées par le Premier ministre, l'action gouvernementale en matière de défense des systèmes d'information ;

– d'animer et de coordonner les travaux interministériels en matière de sécurité des systèmes d'information ;

– d'élaborer les mesures de protection des systèmes d'information proposées au Premier ministre et de veiller à l'application des mesures adoptées

– de mener des inspections des systèmes d'information des services de l'État et d'opérateurs publics ou privés ;

– de mettre en œuvre des dispositifs de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État, des autorités publiques et d'opérateurs publics et privés et de coordonner la réaction à ces événements ;

– de recueillir les informations techniques relatives aux incidents affectant les systèmes d'information de l'État, des autorités publiques et d'opérateurs publics et privés ;

– de délivrer des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ;

– de participer aux négociations internationales et d'assurer la liaison avec ses homologues étrangers ;

– d'assurer la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information.

2. Le dispositif introduit par la commission spéciale

La commission spéciale a adopté l'amendement de M. Arnaud Saint-Martin demandant au gouvernement la remise d'un rapport au Parlement présentant « *les*

(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.

moyens humains et financiers supplémentaires indispensables pour que [l'ANSSI] *puisse contrôler l'application et l'effectivité de la présente loi* ».

Pour son auteur, l'ANSSI risque de manquer de crédits et d'emplois pour mettre en œuvre les dispositions du titre II transposant la directive NIS 2. Il met en avant l'écart de moyen entre ce service et son homologue allemand à titre d'illustration.

*

* *

Article 64 (nouveau)

Demande de rapport sur la mise en œuvre de la stratégie nationale en matière de cybersécurité

Introduit par la Commission spéciale

➢ **Résumé du dispositif et effets principaux**

Cet article additionnel vise à ce que le gouvernement remette un rapport au Parlement sur la mise en œuvre de la stratégie nationale en matière de cybersécurité (cf. article 5 *bis*) précisant les moyens mis à sa disposition pour l'exercice de ses missions de contrôle et d'audit. Le rapport doit également évaluer les besoins à venir au regard de l'élargissement du périmètre des entités concernées par le titre II du projet de loi.

➢ **Dernières modifications législatives intervenues**

(sans objet).

1. L'état du droit

L'article 7 de la directive NIS 2 [(1)] prévoit que « *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* ».

En conséquence, le Sénat a adopté un article additionnel au sein du titre II prévoyant que le Premier ministre élabore une telle stratégie [(2)]. Cet article 5 *bis*

(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.

(2) Cf. commentaire de l'article 5 bis.

prévoit par ailleurs qu'à compter de 2026 et tous les deux ans, le gouvernement remette au Parlement un rapport sur sa mise en œuvre qui précise également l'évolution des indices de performance définis par celle-ci.

2. Le dispositif introduit par la commission spéciale

La commission spéciale a adopté l'amendement de M. René Pilato qui insère un article additionnel demandant au gouvernement la remise d'un rapport au Parlement sur la stratégie nationale en matière de cybersécurité qui précise « *les moyens humains, techniques et financiers mis à sa disposition pour l'exercice de ses missions de contrôle et d'audit* », d'une part, et évalue « *les besoins à venir au regard de l'élargissement du périmètre des entités concernées par la présente loi* ».

LISTE DES PERSONNES AUDITIONNÉES EN COMMISSION PLÉNIÈRE

(par ordre chronologique)

Agence nationale de sécurité des systèmes d'information (ANSSI) (1re audition)

M. Vincent Strubel, directeur général

M. Gaëtan Poncelin de Raucourt, sous-directeur « Stratégie »

Secrétariat général de la défense et de la sécurité nationale (SGDSN)

M. Nicolas Roche, secrétaire général

Table ronde « associations d'élus »

– **Association des maires de France (AMF)**

M. Michel Sauvade, vice-président du conseil départemental du Puy-de-Dôme, maire de Marsac-en-Livradois, co-président de la commission numérique nationale de l'AMF

– **Régions de France**

Mme Constance Nebbula, vice-présidente de la Région Pays de la Loire en charge du numérique et de l'intelligence artificielle

M. Alexandre Ventadour, conseiller territorial de Martinique, chargé du numérique et du développement économique

– **Intercommunalités de France**

Mme Marlène Le Dieu De Ville, vice-présidente en charge du numérique, vice-présidente déléguée à l'économie numérique et aux systèmes d'information et à la culture de la communauté des communes de Lacq-Orthez

Table ronde « autorités de régulation financière »

– **Autorité des marchés financiers (AMF)**

M. Sébastien Raspiller, secrétaire général

– **Autorité de contrôle prudentiel et de résolution (ACPR)**

M. Frédéric Hervo, secrétaire général adjoint

M. Alexandre Garcia, chef de service adjoint du service des affaires internationales

Table ronde « entreprises de cyberdéfense »

– **Airbus ***

M. Michaël Barthellemy, responsable de la gestion des risques cyber et des actifs et représentant de la commission Cyber du Groupement des industries françaises aéronautiques et spatiales (Gifas)

M. Thierry Racaud, président-directeur général d'Airbus Protect

M. Yves Berthe, coordinateur sécurité d'Airbus France

– **Orange Cyberdéfense ***

M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing

M. Vivien Mura, directeur des technologies

– **Tehtris**

Mme Katuiscia Benloukil, vice-présidente communication

– **Sekoia.io**

M. Arnaud Dechoux, directeur des affaires publiques

Table ronde « entreprises de télécommunications »

– **Fédération française des télécoms (FFT) ***

M. Patrick Guyonneau, président de la commission sécurité de la FFT et directeur de la sécurité du groupe Orange

– **Altice France ***

M. Matthieu Hennebo, directeur cybersécurité, responsable sécurité des systèmes d'information (RSSI) du groupe Altice France

M. Corentin Durand, responsable des affaires publiques de Bouygues Telecom

– **Groupe Iliad ***

M. Patrice Millecamps, directeur des obligations légales

Mme Ombeline Bartin, directrice des relations extérieures

Table ronde « experts de la cybersécurité »

– **CyberTaskForce**

M. Sébastien Garnault, fondateur

M. Philippe Luc, membre de Cyber Task Force et président d'Anozr Way

Mme Anne-Élise Jolicard, responsable des affaires publiques d'Anozr Way

– **CyberCercle**

Mme Bénédicte Pilliet, présidente

M. Christian Daviot, senior advisor

M. François Coupez, senior advisor

M. Stéphane Meynet, senior advisor

– **Clusif**

M. Benjamin Leroux, administrateur

M. Michel Dubois, administrateur

Mme Garance Mathias, administratrice

– **Hexatrust**

M. Jean-Noël de Galzain, président

Mme Dorothée Decrop, déléguée générale

– **Alliance pour la confiance numérique (ACN) ***

M. Daniel Le Coguic, président

M. Yoann Kassianides, directeur général

– **Club des experts de la sécurité de l'information et du numérique (Cesin)**

Mme Mylène Jarossay, vice-présidente

M. Arnaud Martin, vice-président

Table ronde « représentants des entreprises »

– **Mouvement des entreprises de France (Medef) ***

Mme Juliette Rouilloux-Sicre, vice-présidente du groupe Thalès, présidente du comité régulation du numérique

Mme Mathilde Briard, chargée de mission économie numérique

Mme Marie David, chargée de mission affaires publiques

– **Confédération des petites et moyennes entreprises (CPME) ***

M. Franck Bataille, membre du comité exécutif en charge du numérique et de l'innovation

M. Marc Bothorel, référent cybersécurité

Mme Léa Bouchet, juriste commerce et consommation

M. Adrien Dufour, responsable affaires publiques

Commission nationale de l'informatique et des libertés (CNIL)

M. Michel Combot, directeur des technologies, de l'innovation, et de l'intelligence artificielle

M. Victor Nicolle, directeur des contrôles et des sanctions

M. Florent Della Valle, chef du service de l'expertise technologique

Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles

Table ronde « lutte contre la cybercriminalité »

– **Groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma)**

M. Jérôme Notin, directeur général

– **Ministère de l'intérieur dans le cyberespace (Comcyber-MI)**

M. Christophe Husson, général de division et chef du Comcyber-MI

– **Parquet de Paris**

Mme Johanna Brousse, vice-procureure, cheffe de la section J3 (lutte contre la cybercriminalité)

Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep)

Mme Laure de La Raudière, présidente

M. Olivier Corolleur, directeur général

Table ronde « chiffrement n° 1 »

– **Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT)**

M. Mahamadou Diarra, secrétaire général

– **Groupement interministériel de contrôle (GIC)**

M. Pascal Chauve, directeur

– **Direction générale de la sécurité intérieure (DGSI)**

Mme Céline Berthon, directrice générale

Table ronde « chiffrement n° 2 »

– **Société Olvid**

M. Thomas Baignères, docteur en cryptographie, co-fondateur de la société Olvid

M. Matthieu Finiasz, docteur en cryptographie, co-fondateur de la société Olvid

– **Mozilla**

M. Benjamin Beurdouche, chercheur en ingénierie de sécurité et de confidentialité

Agence nationale de sécurité des systèmes d'information (ANSSI) (2e audition)

M. Vincent Strubel, directeur général

** Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique.*

LISTE DES PERSONNES AUDITIONNÉES PAR MME CATHERINE HERVIEU, RAPPORTEURE SUR LE TITRE IER

(par ordre chronologique)

Direction générale de l'armement (DGA)

M. l'ingénieur général de l'armement Pascal Fintz, chef du service de la sécurité de défense et des systèmes d'information

M. Mathieu Jacquart, chef du bureau de la protection et de la réglementation

Direction de la protection des installations, moyens et activités de la défense (DPID)

M. le général de division aérienne Nicolas Leverrier, directeur de la protection des installations, moyens et activités de la défense

M. le colonel Cyrille Caron, responsable politique de protection de la DPID

FP2E*

M. Mathias Largillière, cybersécurité et protection des données, Saur

M. Thomas Billaut, responsable « Cyber Factory », Suez

M. Christophe Maissa, référent national sûreté, direction technique, Suez

M. Jean-Paul Courcier, coordinateur national gestion d'alerte et de crise, correspondant « Sûreté Eau France », Veolia

M. Matthieu Bertin, responsable de la sécurité des systèmes d'information, Veolia

Mme Aurélie Colas, déléguée générale, FP2E

Mme Sara Djabali, conseillère « affaires publiques », FP2E

FEDENE*

M. Pascal Guillaume, président

Mme Marion Lettry, déléguée générale

M. Bertrand Nachbaur, président de FEDENE Solutions Numériques

M. Louis Lesigne, conseil « affaires publiques »

France Hydrogène*

M. Philippe Boucly, président

M. Guillaume Buttin, chargé de mission « relations institutionnelles »

Audition conjointe

– Ministère de l'Économie, des finances et de la souveraineté industrielle et numérique – Secrétariat général des ministères économiques et financiers

Mme Anne Blondy-Touret, secrétaire générale des ministères économiques et financiers, haute fonctionnaire de défense et de sécurité (HFDS)

M. Samuel Heuzé, haut fonctionnaire de défense et de sécurité adjoint

– Ministère de la transition écologique, de la biodiversité, de la forêt, de la mer et de la pêche - Secrétariat général

M. Guillaume Leforestier, haut fonctionnaire de défense et de sécurité (HFDS)

Mme Nathalie Gayral, cheffe de service (HFDS)

Préfecture de la région Grand

M. Matthieu Ringot, préfet délégué pour la zone de défense et de sécurité auprès du préfet de la région Grand Est

Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)

M. Gwenaël Jezequel, conseiller relations institutionnelles et communication auprès du secrétaire général

M. Alexandre Nègre, conseiller juridique auprès du secrétaire général

M. Arthur Danin, chef du bureau de la résilience interministérielle

SNCF*

M. Xavier Roche, directeur de la sûreté du groupe SNCF

M. Jean-Christophe Mathieu, directeur de la sécurité numérique du groupe SNCF

M. Jean-Luc Planchet, responsable défense et sécurité de SNCF Réseau

M. Yann Keribin, responsable défense et sécurité de SNCF Gares&Connexions

Mme Laurence Nion, conseillère parlementaire du groupe SNCF.

** Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique.*

LISTE DES PERSONNES AUDITIONNÉES PAR MME ANNE LE HÉNANFF, RAPPORTEURE SUR LE TITRE II

(par ordre chronologique)

Thales

M. Alexis Caurette, vice-président « Stratégie Cybersécurité »

Mme Isabelle Caputo, vice-présidente « Relations institutionnelles

Mme Alexandra Iteanu, avocate

Association française pour le nommage internet en coopération (AFNIC)

M. Pierre Bonis, directeur général

M. Lucien Castex, conseiller du directeur général Internet Gouvernance et Société

Table ronde « entreprises extra européennes »

– **Amazon Web Services (AWS)**

M. Cédric Mora, Public Policy Manager France – Cybersécurité/IA

M. Stephan Hadinger, Head of Technology France

– **Google**

M. Thiébaut Meyer, directeur « cybersécurité »

M. Frédéric Géraud de Lescazes, directeur des relations institutionnelles

– **Microsoft**

M. Arnaud Jumelet, chef de programme Cybersécurité

M. Lionel Benatia, directeur des affaires publiques

– **Apple**

M. Bruno Bernard, Senior Manager, Government Affairs Europe

– **Huawei**

M. Minggang Zhang, directeur général adjoint

Mme Myriam Lagarde, directrice des affaires institutionnelles

Table ronde « clouders »

– **Cloud Temple**

M. Giuliano Ippoliti, directeur de la cybersécurité

– **OVHcloud**

M. Julien Levrard, responsable de la sécurité des systèmes d'information

Mme Elisa Sharps, responsable des affaires publiques

– **OUTSCALE**

M. Grégory Abate, secrétaire général de Dassault Systèmes

M. David Chassan, Chief Strategy Officer

Table ronde « cabinets de conseil »

– **Wavestone**

M. Gérôme Billois, Partner

– **One Point**

M. Alexis Bouin, Leader Cybersecurité

M. Fabrice Groseil, Partner Cybersecurité

– **Ernst & Young**

M. Marc Ayadi, Partner

M. Fabrice Naftalski, avocat associé

Table ronde « santé »

– **Agence du Numérique en Santé (ANS)**

M. Jean-Baptiste Lapeyrie, directeur Expertise, innovation et international

– **Association Pour la Sécurité des Systèmes d'Information de Santé (Apssis)**

M. Vincent Trély, président-fondateur

– **Syndicat national de l'industrie des technologies médicales (Snitem)**

Mme Cécile Vaugelade, directrice des affaires réglementaires

M. Arnaud Augris, responsable des affaires réglementaires

– **Club RSSI Santé**

M. Jean-Sylvain Chavanne, responsable de la sécurité des systèmes d'information du CHU de Brest et du GHT de Bretagne Occidentale

UGAP

M. François Lafond, directeur général adjoint en charge du numérique

Table ronde « chiffrement »

– **Meta**

M. Anton'Maria Battesti, directeur des affaires publiques France

Mme Aurore Denimal, responsable des affaires publiques France

– **Olvid**

M. Thomas Baignères, co-fondateur, président-directeur-général

M. Cédric Sylvestre, co-fondateur, vice-président business développement

Table ronde « CSIRT / CERT »

– **CSIRT Bretagne - Breizh Cyber**

M. Guillaume Chéreau, directeur de Breizh Cyber

– **CSIRT Santé**

M. Steven Garnier, directeur du domaine cybersécurité

– **CSIRT Normandie Cyber**

M. Stéphane Bresson, responsable du département « Normandie Cyber »

– **CSIRT Maritime – France Cyber Maritime**

M. Xavier Rebour, directeur

– **CERT Aviation France**

M. Marc Leymonerie, président

GIP ACYMA

M. Jérôme NOTIN, directeur général

Table ronde « associations d'élus »

– **Association des maires de France (AMF)**

M. Patrick Molinoz, vice-président, co-président de la commission « numérique », maire de Venarey-Lès-Laumes

Mme Véronique Picard, chargée de mission « numérique »

Mme Marie-Cécile Georges, responsable du département « intercommunalités et territoire »

– **Intercommunalités de France**

Mme Marlène Le Dieu de Ville, vice-présidente en charge du numérique

M. Jules Podsczaski, conseiller « numérique »

Mme Montaine Blonsard, responsable des relations avec le Parlement

Table ronde « éditeurs de logiciels »

– **Berger-Levrault**

M. Jérôme Bonnet, directeur de la technologie, membre du Comex

M. Stéphane Manou, directeur général collectivités France, membre du Comex et élu local

– **Arpège**

M. Nathanaël Veron, RSSI

– **Arche MC2**

M. Guillaume Bouillot, président

M. Tristan Prophète, responsable de la sécurité des systèmes d'information

Stoïk

M. Jules Veyrat, président-directeur général

M. Vincent Nguyen, directeur de la cybersécurité

** Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique.*

LISTE DES PERSONNES AUDITIONNÉES PAR M. MICKAËL BOULOUX, RAPPORTEUR SUR LE TITRE III

(par ordre chronologique)

Direction générale du Trésor

Mme Camille Sutter, cheffe du pôle des affaires internationales, de la coordination européenne et des enjeux technologiques du secteur financier (PAIET) au service du financement de l'économie (SFE) ;

M. Paul Abadie, adjoint à la cheffe du PAIET ;

M. Victor Millard, adjoint à la cheffe du bureau « entreprises et intermédiaires d'assurance » à la sous-direction des assurances et de l'économie sociale et solidaire du SFE ;

M. Jordan Granata, adjoint au chef du bureau « affaires bancaires » à la sous-direction des banques et des financements d'intérêt général du SFE

M. Thomas Durantet, adjoint au conseiller juridique ;

M. Sofien Abdallah, conseiller parlementaire et relations institutionnelles.

Table ronde regroupant des adhérents de l'Association française des établissements de crédit et des entreprises d'investissement (AFECEI)

– Association française des marchés financiers (AMAFI)

Mme Stéphanie Hubert, directrice générale

– Fédération bancaire française

M. François Lefebvre, directeur général adjoint

M. Jérôme Pardigon, directeur du département « Relations institutionnelles France Stratégie, communication, adhérents »

– BNP Paribas

M. Thierry Markwitz, responsable du programme DORA pour BNP Paribas

– Association française des établissements de paiement et de monnaie électronique

M. Alexandre Tribolet, *Head Regulatory* de Qonto

France Assureurs

Mme Mélodie Leloup-Velay, directrice « droit et conformité »

M. Isma Haffad, responsable d'études juridiques

M. Arnaud Giros, responsable des affaires parlementaires et gouvernementales